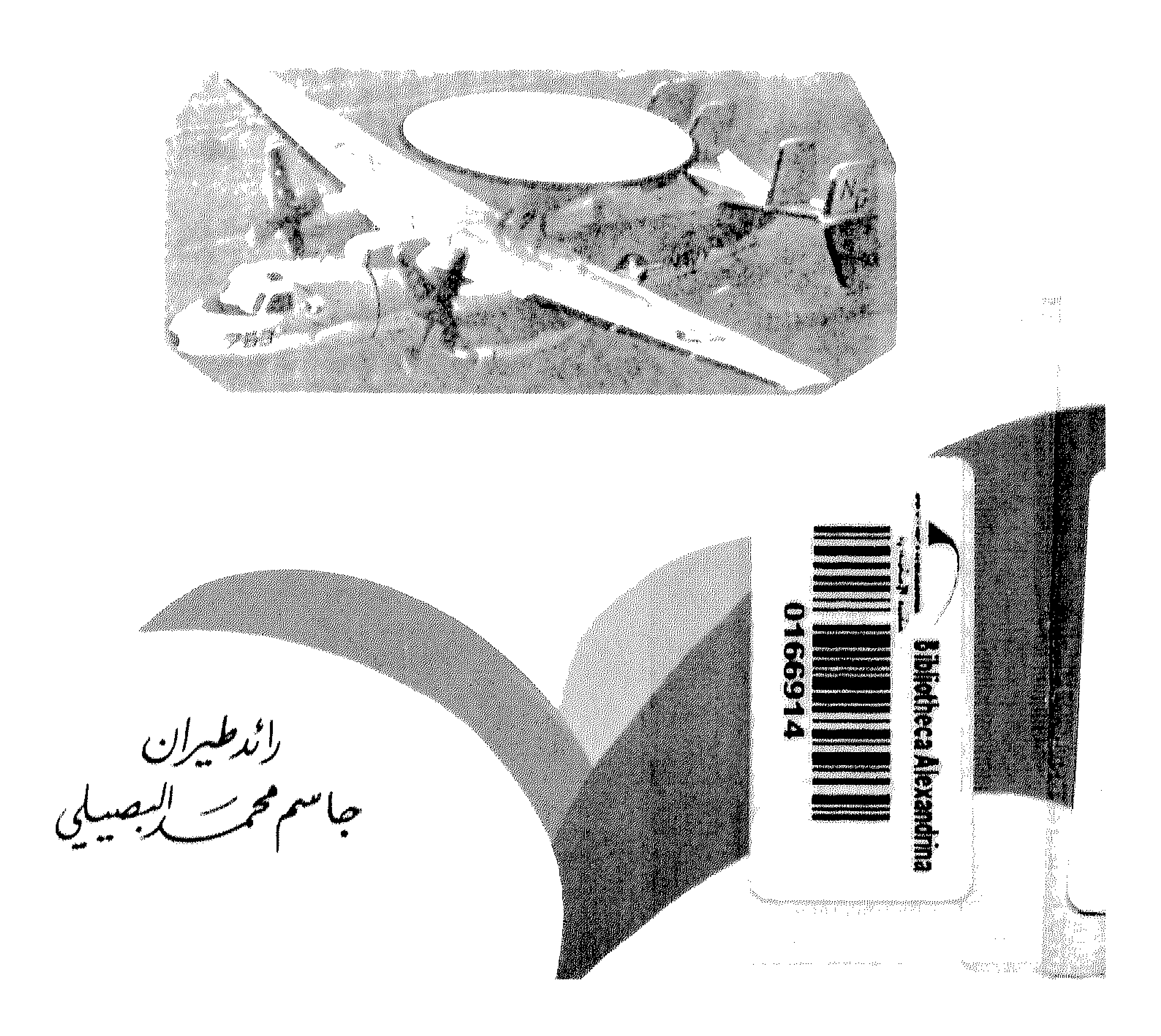
المؤسسة
العربية
للدراسات
والنشر

الحرب الألكترونية

اسسها وأثرها في الحروب



رائد طيران
جاسم محمد البصيلي

الحرب الإلكترونية

أسسها وأثرها في الحروب

المؤسسة العربية
للدراسات والنشر
بناية برج الكارلتون ـ ساقية الجنزير ـ
ت ١/٨٠٧٩٠٠ برقياً : موكيالي ؛
بيروت ـ ص.ب : ٥٤٦٠/١١ بيروت
تلكس LE DIRKAY ـ ٤٠٠٦٧

الطبعة الثانية ١٩٨٩ م

الحرب الألكترونية

اسسها وأثرها في الحروب

رائد طيران : جاسم محمد البصيلي

مراجعة الدكتور: مالك غلوم حسين
جامعة الكويت

المؤسسة
العربية
للدراسات
والنشر

الفهرس

الصفحة

الباب الثالث

الباب الرابع:

بسم الله الرحمن الرحيم

المقدمة

إن الحمد لله نحمده ونستعينه ونستغفره ونعوذ بالله من شرور أنفسنا ومن سيئات أعمالنا من يهده الله فلا مضل له ومن يضلل فلا هادي له. وأشهد أن لا إله إلا الله وحده لا شريك له وأن محمدا عبده ورسوله.

أما بعد فانطلاقا من قول الله عز وجل: ﴿**يأيها الذين آمنوا خذوا حذركم فانفروا ثبات أو انفروا جميعا**﴾ ومن قوله تعالى: ﴿**وأعدوا لهم ما استطعتم من قوة ومن رباط الخيل ترهبون به عدو الله وعدوكم**﴾ وامتثالا بقوله تعالى: ﴿**ولا تلقوا بأيديكم إلى التهلكة**﴾ وقول الرسول ﷺ: «المؤمن القوي خير وأحب إلى الله من المؤمن الضعيف». فإني عزمت على كتابة هذا الكتاب وذلك لما لمست من الحاجة الماسة إليه ومن عدم الاهتمام بهذا الموضوع وهو الحرب الالكترونية وهذا إن دل على شيء إنما يدل على مدى تهاوننا وعدم تقديرنا الصحيح لهذا الموضوع واستهتارنا بعدونا وأعداء الأمة الإسلامية الكثيرين وأخص هنا بالذكر الكيان الصهيوني الممسوخ الذي هو في حقيقته وليد غير شرعي لأعداء الإسلام والأمة العربية ولكنه ـ للأسف ـ يعتبر من الدول المتقدمة في هذا النوع من الحرب.

وكان لانتصاراته علينا أسباب عديدة وليست بخافية على أحد ولكن الذي أريد أن أنبه إليه أخواني في الإسلام هو هذا الموضوع الخطير الذي ستتضح خطورته أكثر عند قراءة هذا الكتاب وما ورد فيه من أمثلة واقعية مرة.

ورغم أن هذا الموضوع فيه الكثير من التعقيد والتشابك بين فروعه المختلفة، فإني بذلت جهدي، وحاولت قدر طاقتي أن أبسطه من التعقيد بحيث يكون في مقدور القارىء الكريم أن يعيه الوعي كله. وتعمدت أن لا أتعمق في طرح أسس الحرب الإلكترونية حتى لا يتسرب الملل إلى نفس القارىء، (**ويجب إعتبار هذا الكتاب مجرد مقدمة ومعلومة وليس كمرجع ، وكلنا ثقة أن الرجال القائمين على موضوع الحرب**

الإلكترونية في الدول العربية والإسلامية سيكتبون ما هو أدق وأشمل كمرجع لنا من واقع خبراتهم الطويلة) .

ونسأل الله تعالى أن يجزي كل من ساهم في اخراج هذا الكتاب بصورته النهائية خير الجزاء، كما نسأله سبحانه أن ينفع به كل الساعين إلى ما فيه خير الإسلام .

والحمد لله رب العالمين

رائد طيران
جاسم محمد البصيلي

الباب الأول

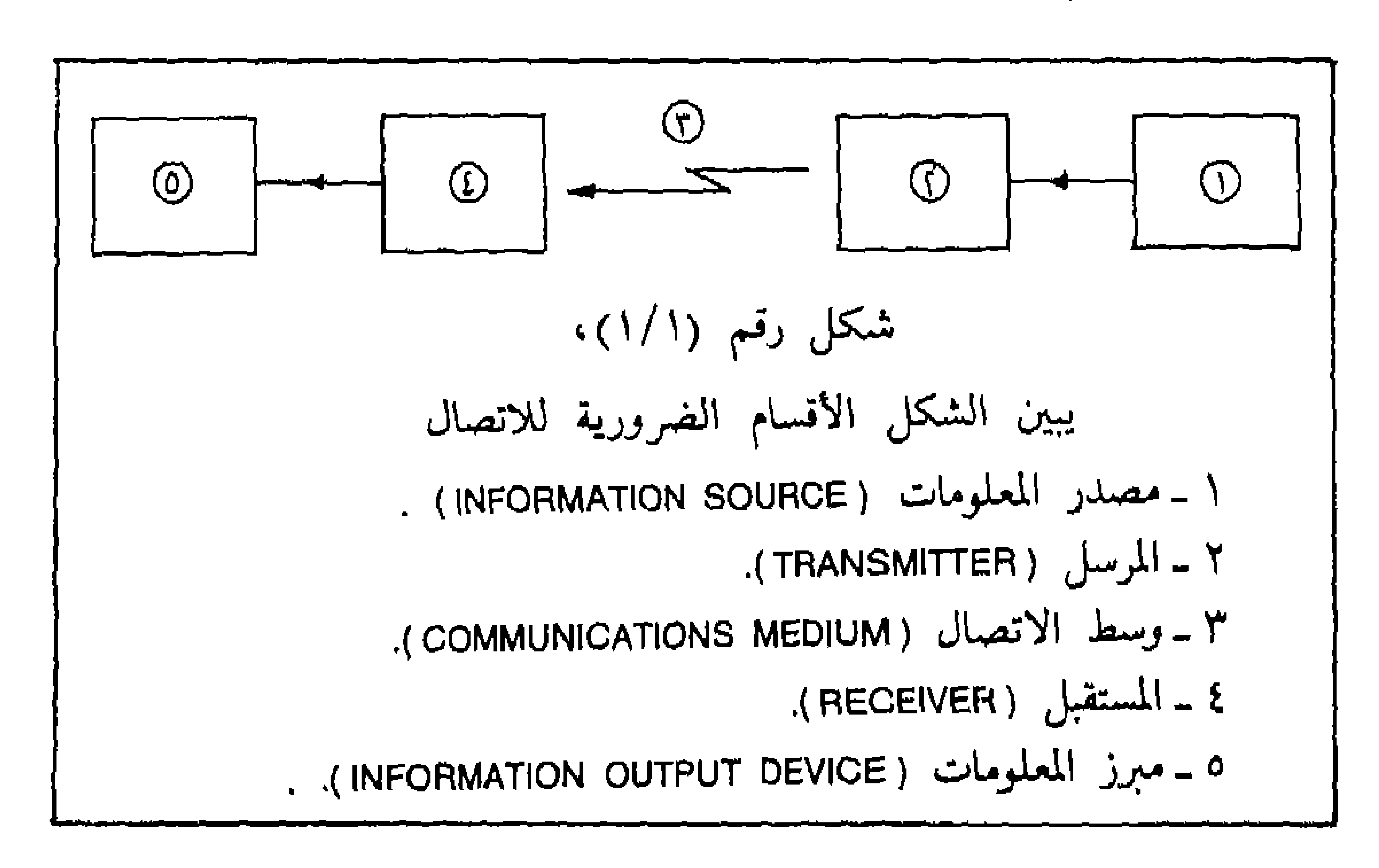
تمهيد ومدخل للبحث

١ ــ مختصر نظم الاتصالات والرادار والذبذبات

سنبدأ أولا بالتحدث عن موضوع نظم الإتصالات والرادار والذبذبات بصورة عامة ومختصرة حتى نمهد للقارىء سهولة تقبل فكرة موضوع الحرب الإلكترونية، وذلك لأننا قد إستخدمنا نظم الإتصالات والرادار والذبذبات في شرح أسس الحرب الإلكترونية في الكتاب.

أ ــ الإتصالات :

نظام الاتصالات بين جهة وأخرى أو بين شخص وآخر يجب أن يتكون من : مصدر المعلومات والمرسل، ووسط الاتصال ثم المستقبل، ومبرز المعلومات. (أنظر شكل رقم ١/١) .



شكل رقم (١/١)،

يبين الشكل الأقسام الضرورية للاتصال

١ ـ مصدر المعلومات (INFORMATION SOURCE) .

٢ ـ المرسل (TRANSMITTER).

٣ ـ وسط الاتصال (COMMUNICATIONS MEDIUM).

٤ ـ المستقبل (RECEIVER).

٥ ـ مبرز المعلومات (INFORMATION OUTPUT DEVICE). .

هذه الأقسام الخمسة هي المكونات الأساسية لأي نظام اتصال مهما كان نوعه. فنظام الاتصال الذي يعتمد على الأجهزة الإلكترونية، يكون (مصدر المعلومات) هذا هو القسم الذي يحول المعلومات المراد إرسالها إلى إشارات كهربائية (ELECTRICAL SIGNALS) مثل جهاز الميكروفون أو جهاز التلكس أو جهاز الفاكسمل . . الخ .

تنتقل الإشارات الكهربائية هذه إلى قسم المرسل وهو جهاز إرسال يقوم بتحويل تلك المعلومات التي هي على شكل إشارات كهربائية إلى إشارات مناسبة لبثها أو إرسالها عبر وسط الاتصال المتفق عليه بين المرسل والمستقبل.

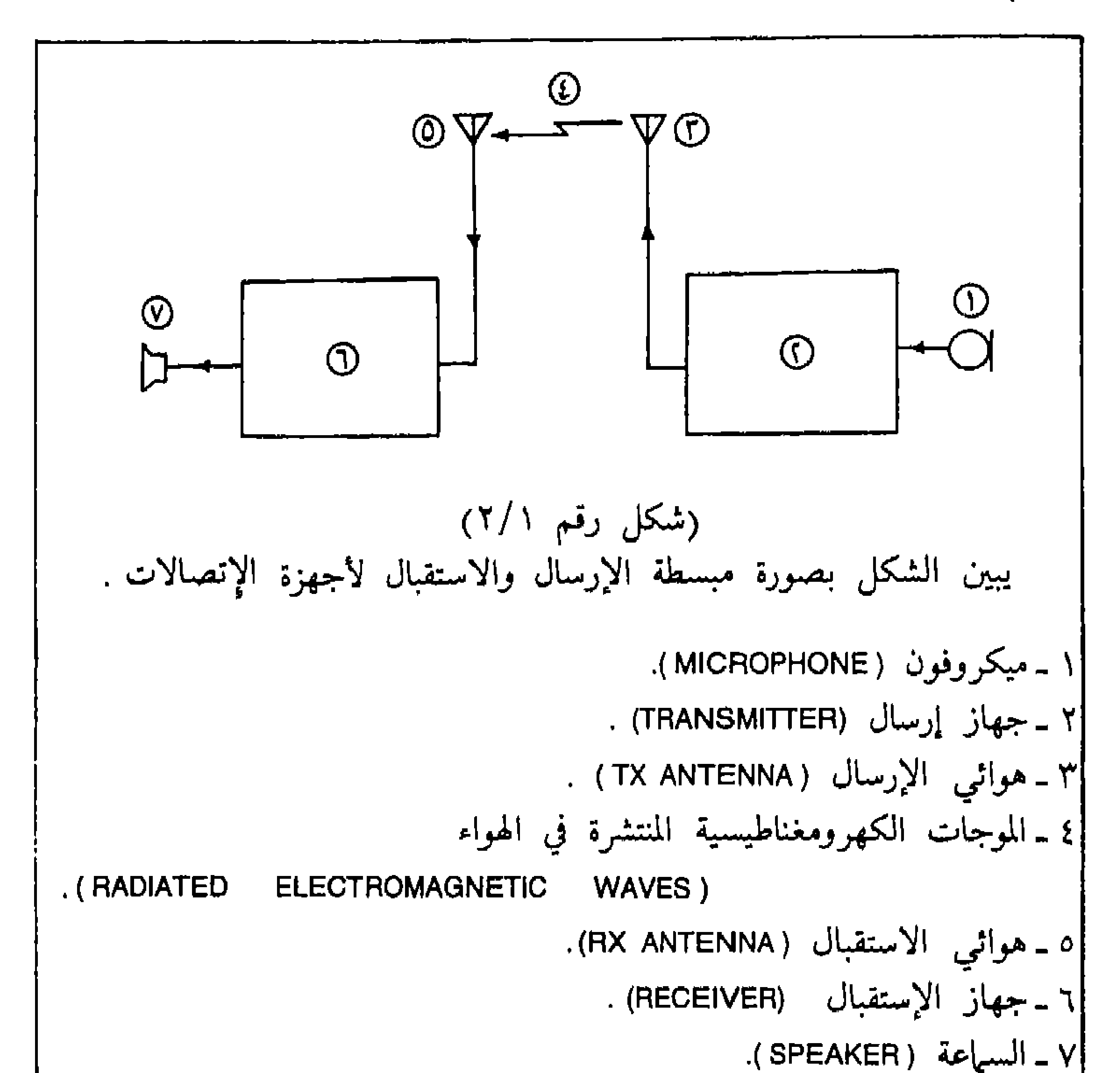
وسط الاتصال (COMMUNICATIONS MEDIUM) هو ما بين جهاز الإرسال وجهاز الاستقبال تنتقل فيه المعلومات على هيئة إشارات (SIGNALS) فمثلا:

- إذا كان وسط الاتصال سلك أو كيبل (WIRE OR CABLE) تكون المعلومات على هيئة إشارات كهربائية (ELECTRICAL SIGNALS) .
- وإذا كان وسط الاتصال الهواء الخارجي (ATMOSPHERE) تنتقل المعلومات على هيئة إشارات كهرومغناطيسية (ELECTROMAGNETIC SIGNALS) .
- وإذا كان وسط الاتصال هو الماء تنتقل المعلومات على هيئة إشارات صوتية (SOUND SIGNALS) وهكذا .

وسط الاتصال هذا هو الحيز الذي تعتمد عليه معظم عمليات الحرب الإلكترونية كما سنرى وخاصة في الأساس الأول والثاني والثالث. إذ من هذا الوسط تستطيع التقاط إشارات المعلومات المرسلة المنبعثة من أجهزة الارسال ومن ثم رصدها ومعرفة محتواها، وكذلك التشويش على جهاز الاستقبال عبر ذلك الوسط. كما أن معظم أنواع التداخل (INTERFERENCE) - أنظر صفحة ١١٢ - والضجيج (NOISE) تؤثر على أجهزة الاستقبال تأتي عبر وسط الاتصال.

جهاز الاستقبال يقوم باستقبال المعلومات والتي هي على هيئة إشارات فيقوم بتحليلها وتحويلها إلى إشارات كهربائية ثم ترسل إلى مبرز المعلومات التي يبرزها للجهة أو للشخص المستقبل، إبراز المعلومات هنا إما أن يكون على هيئة صوت مسموع باستخدام مبرز المعلومات (سماعة) أو على هيئة ورقة مكتوب عليها المعلومات باستخدام (جهاز تلكس) . . . الخ .

ولنضرب مثالا على ذلك باستخدام جهاز الراديو للاتصال. (أنظر شكل رقم ١/٢).



(شكل رقم ١/٢)

يبين الشكل بصورة مبسطة الإرسال والاستقبال لأجهزة الإتصالات .

١ ـ ميكروفون (MICROPHONE).
٢ ـ جهاز إرسال (TRANSMITTER) .
٣ ـ هوائي الإرسال (TX ANTENNA) .
٤ ـ الموجات الكهرومغناطيسية المنتشرة في الهواء
(RADIATED ELECTROMAGNETIC WAVES).
٥ ـ هوائي الاستقبال (RX ANTENNA).
٦ ـ جهاز الإستقبال (RECEIVER) .
٧ ـ السماعة (SPEAKER).

يتكلم المرسل فيحول الميكروفون الكلام إلى ذبذبات كهربائية إلى جهاز الإرسال الذي يحولها إلى هوائي الارسال فتنبعث على هيئة إرسالية كهرومغناطيسية عبر الهواء الخارجي فيستقبلها هوائي الاستقبال ثم إلى جهاز الاستقبال ثم إلى السماعة التي تحولها إلى موجات صوتية يستجيب لها المستقبل فيفهمها .

وتنقسم نظم الاتصالات بصفة عامة إلى نوعين:

أ ـ اتصالات لاسلكية (WIRELESS COMMUNICATIONS) وهي أن وسط الاتصال

(MEDIA) الذي بين المرسل والمستقبل يكون الهواء الخارجي (الأثير) مثلا فتنتقل فيه المعلومات على هيئة إرساليات كهرومغناطيسية ELECTROMAGNETIC). RADIATIONS OR EMISSIONS).

ب ـ اتصالات سلكية (WIRE COMMUNICATIONS) وهي أن وسط الاتصال الذي بين المرسل والمستقبل يكون سلك (WIRE) فتنتقل فيه المعلومات على هيئة إشارات كهربائية (ELECTRICAL SIGNALS).

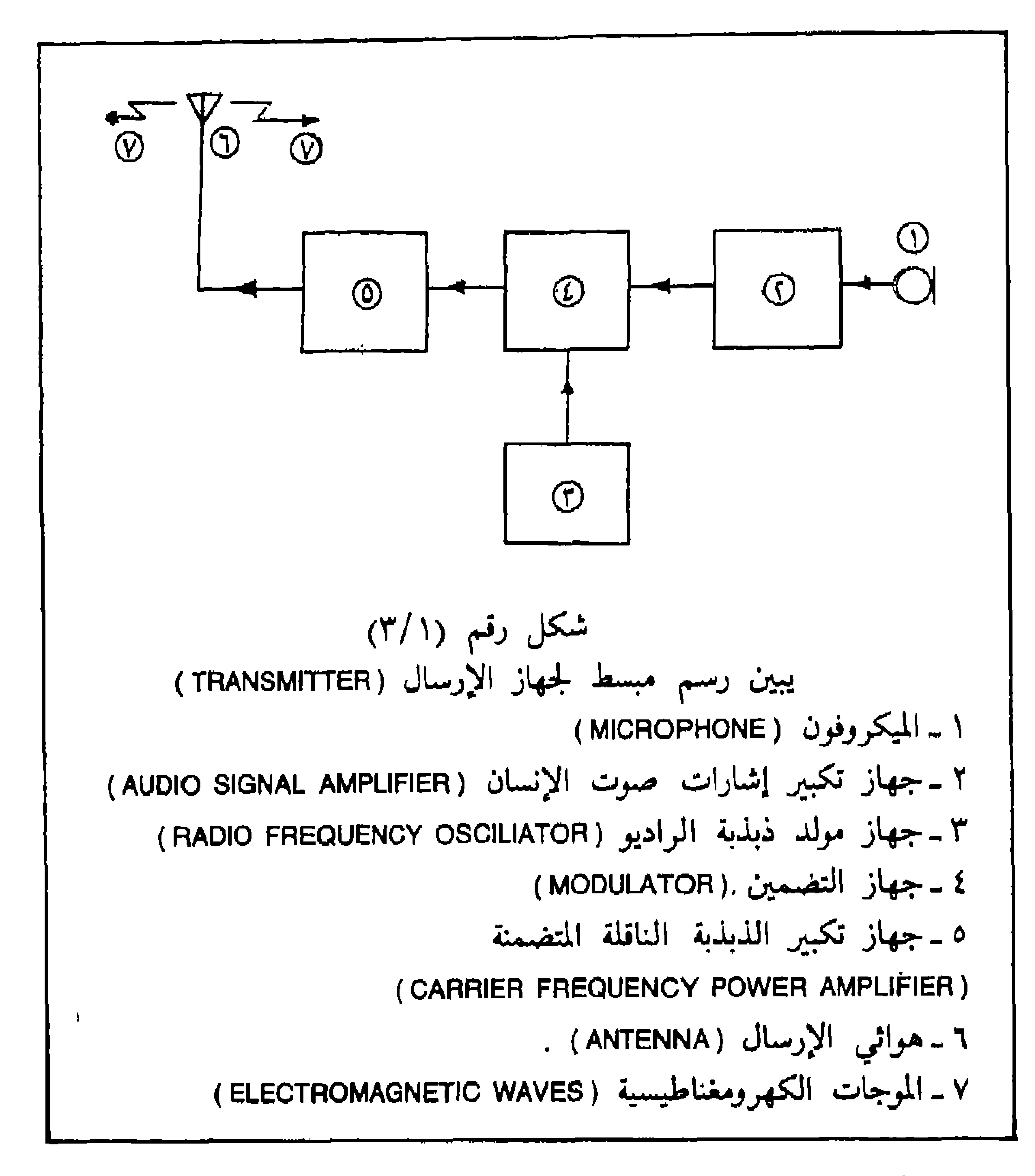
هنا إذا حدث أن التقط شخص آخر تلك المحادثة السابقة وأراد التحدث في نفس الوقت الذي فيه المستقبل يكون في حالة استماع، وكان صوت ذلك الشخص عالي جدا وغير مفهوم حجب ذلك عن المستقبل سماع المرسل وفهم كلامه، أما إذا كان صوت ذلك الشخص بقدر مناسب مقلدا صوت المرسل وفيه معلومات خاطئة مثلا، سوف يسمع المستقبل كلام الشخص وقد يستجيب لتلك المعلومات ويقوم باجراء خاطىء، وهنا كذلك إذا أدرك المستقبل أن هناك شخص غريب يقوم بالتأثير على محادثته مع المرسل بصورة غير مرضية وعدائية، فيقوم عندئذ بتدارك الأمر ويحاول التخلص من ذلك التأثير وحماية محادثته مع المرسل.

وهذه هي فكرة الحرب الإلكترونية من التقاط وتأثير وحماية.

١ ـ جهاز إرسال الراديو **(RADIO TRANSMITTER)**

أنظر شكل رقم (١/٣)

فنرى هنا صوت الإنسان يتحول إلى إشارات كهربائية صوتية تسمى ELECTRIC) AUDIO SIGNALS) هذا التحويل يحدث في الميكروفون ثم تنتقل بعد ذلك للتكبير بجهاز تكبير الصوت (AUDIO SIGNAL AMPLIFIER) ثم تحمل على الذبذبة الناقلة الناتجة عن جهاز مولد الذبذبة الناقلة أو يسمى مولد ذبذبة الراديو CARRIER FREQUENCY) OSCILLATOR OR RADIO FREQUENCY OSCILLATOR) عن طريق جهاز يسمى جهاز التضمين (MODULATOR) ثم بعد ذلك يكبر الناتج بجهاز (POWER AMPLIFIER) لزيادة القدرة على الارسال ثم ترسل الذبذبة الناقلة المتضمنة صوت الانسان إلى الهوائي يعرف بـ (ANTENNA OR AERIAL) وهو الجهاز الذي يستطيع أن يحول تلك الذبذبة من كهربائية سلكية (أي التي تنتقل عبر الأسلاك الكهربائية) إلى إشارة لاسلكية (WIRELESS SIGNAL) فتستطيع أن تنتقل في الهواء الخارجي عبر الأثير وتسمى إرسالية



شكل رقم (١/٣)

يبين رسم مبسط لجهاز الإرسال (TRANSMITTER)

١ ـ الميكروفون (MICROPHONE)

٢ ـ جهاز تكبير إشارات صوت الإنسان (AUDIO SIGNAL AMPLIFIER)

٣ ـ جهاز مولد ذبذبة الراديو (RADIO FREQUENCY OSCILIATOR)

٤ ـ جهاز التضمين (MODULATOR).

٥ ـ جهاز تكبير الذبذبة الناقلة المتضمنة

(CARRIER FREQUENCY POWER AMPLIFIER)

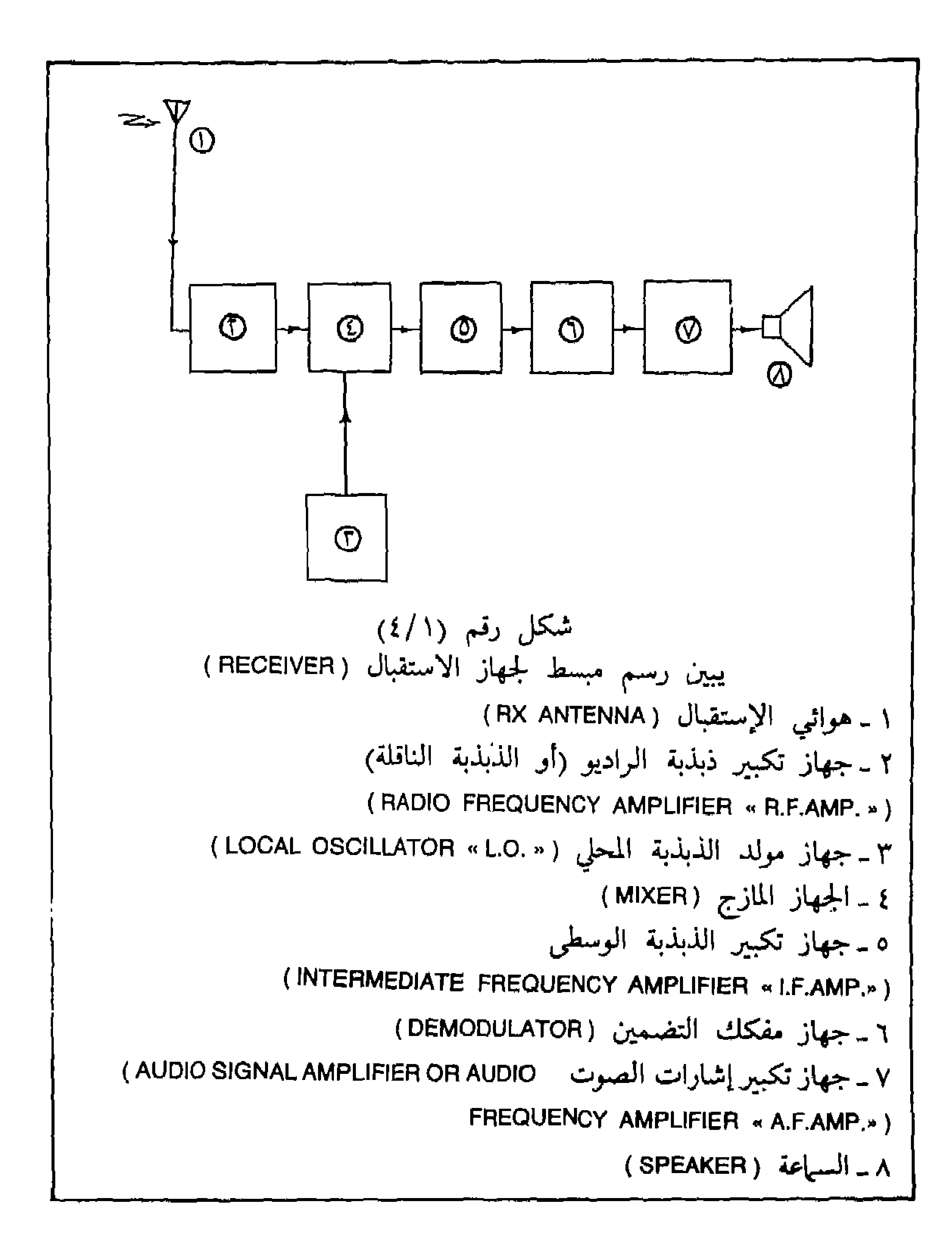
٦ ـ هوائي الإرسال (ANTENNA) .

٧ ـ الموجات الكهرومغناطيسية (ELECTROMAGNETIC WAVES)

كهرومغناطيسية (ELECTROMAGNETIC RADIATION OR EMISSION) تنتقل بسرعة الضوء إلى حوالي ٣٠٠,٠٠٠ كم/ الثانية.

٢ ـ جهاز استقبال الراديو سوبر هترودايان (SUPER HETERODYNE RECEIVER)
أنظر شكل رقم (٤/١)

يستقبل الإرسال الكهرومغناطيسي من قبل الهوائي ليكبر بجهاز تكبير الذبذبة الناقلة أو ذبذبة الراديو (RADIO FREQUENCY AMPLIFIER OR CARRIER FREQUEN-



شكل رقم (١/٤)

يبين رسم مبسط لجهاز الاستقبال (RECEIVER)

١ ـ هوائي الإستقبال (RX ANTENNA)

٢ ـ جهاز تكبير ذبذبة الراديو (أو الذبذبة الناقلة)
(RADIO FREQUENCY AMPLIFIER « R.F.AMP. »)

٣ ـ جهاز مولد الذبذبة المحلي (« LOCAL OSCILLATOR « L.O.)

٤ ـ الجهاز المازج (MIXER)

٥ ـ جهاز تكبير الذبذبة الوسطى
(INTERMEDIATE FREQUENCY AMPLIFIER « I.F.AMP.»)

٦ ـ جهاز مفكك التضمين (DEMODULATOR)

٧ ـ جهاز تكبير إشارات الصوت (AUDIO SIGNAL AMPLIFIER OR AUDIO
FREQUENCY AMPLIFIER « A.F.AMP.»)

٨ ـ السماعة (SPEAKER)

CY AMPLIFIER) ثم ترسم إلى المازج (MIXER) الذي تأتيه ذبذبة من مولد الذبذبات المحلي (LOCAL OSCILLATOR) الذي عادة ذبذبته أكبر من الذبذبة الناقلة بقليل، وبعد

المزج تنتج ذبذبة تسمى الذبذبة الوسطى (INTERMEDIATE FREQUENCY) التي عادة تكون حوالي ٤٥٤ كيلو هرتز أو حسب تصميم جهاز الراديو.

بعد ذلك تكبر الذبذبة بجهاز (INTERMEDIATE FREQUENCY AMPLIRIER) ثم ترسل إلى مفكك التضمين ويسمى (DETECTOR OR DEMODULATOR) فيكون الناتج هو ذبذبات صوت الانسان المرسل فتكبر بجهاز تكبير الصوت (AUDIO FREQUENCY AMPLIFIER) وترسل إلى السماعة ليسمعها الإنسان المستقبل.

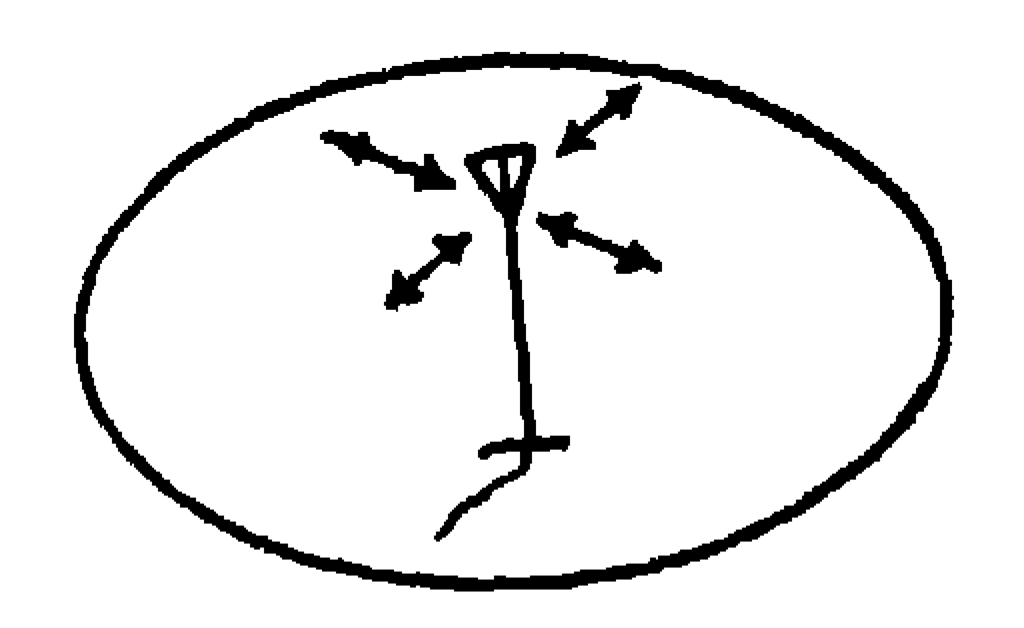
هناك طرق عدة للتضمين (MODULATION) منها :

أ ـ تضمين الاتساع (AMPLITUDE MODULATION) وهو أن وسع أو مقدار الذبذبة الناقلة يتغير بتردد أو بذبذبة صوت الإنسان.

ب ـ تضمين التردد (FREQUENCY MODULATION) وهو أن تردد أو ذبذبة الذبذبة الناقلة يتغير بتردد أو ذبذبة صوت الإنسان.

معظم الهوائيات تستخدم للإرسال وتستخدم كذلك للاستقبال وهناك نوعين من الهوائيات :

أ ـ هوائي لجميع الجهات ويعرف بـ (OMNIDIRECTIONAL ANTENNA) وهذا تكون كل طاقة إرساله ومدى استقباله لجميع الجهات ٣٦٠°. انظر شكل رقم (١/٥).

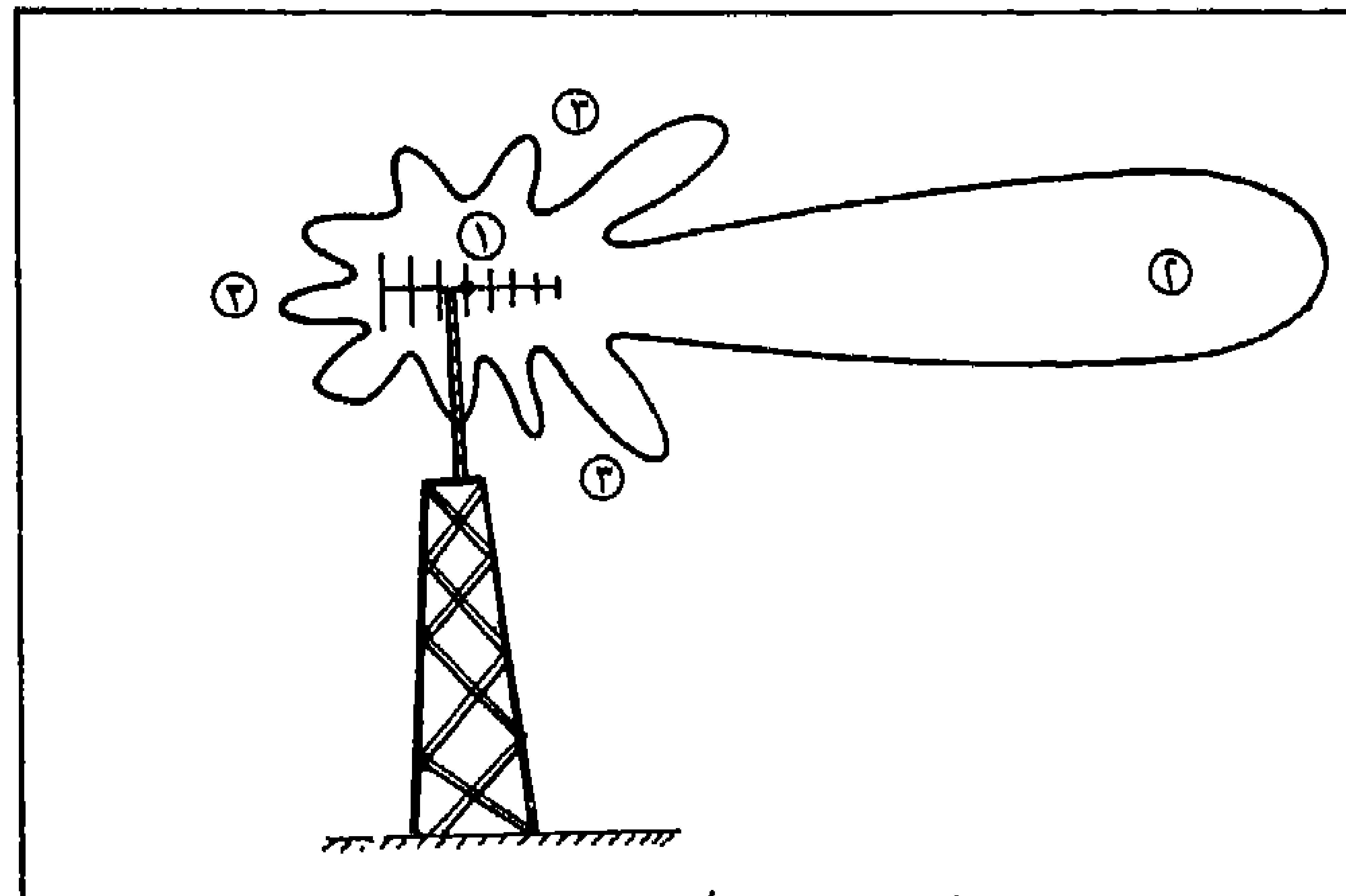


شكل رقم (١/٥)يبين في الوسط

هوائي لجميع الاتجاهات (OMNI-DIRECTIONAL ANTENNA) والدائرة تعبر عن مدى وتغطية جميع الإتجاهات بالتساوي من حيث الإرسال والإستقبال.

ب ـ هوائي فقط لجهة واحدة ويعرف بـ (DIRECTIONAL ANTENNA) وهذا تكون معظم طاقة إرساله ومدى استقباله فقط من جهة أو جزء أو زاوية معينة ومجال ومدى تلك الطاقة تسمى الشعاع الرئيسي (MAIN BEAM OR LOBE) وباقي طاقة الارسال والاستقبال تتوزع على عدة أشعة جانبية (SIDE BEAMS OR LOBES) وتلك الأشعة الجانبية تكون ذات مدى غير بعيد في الإرسال والاستقبال.

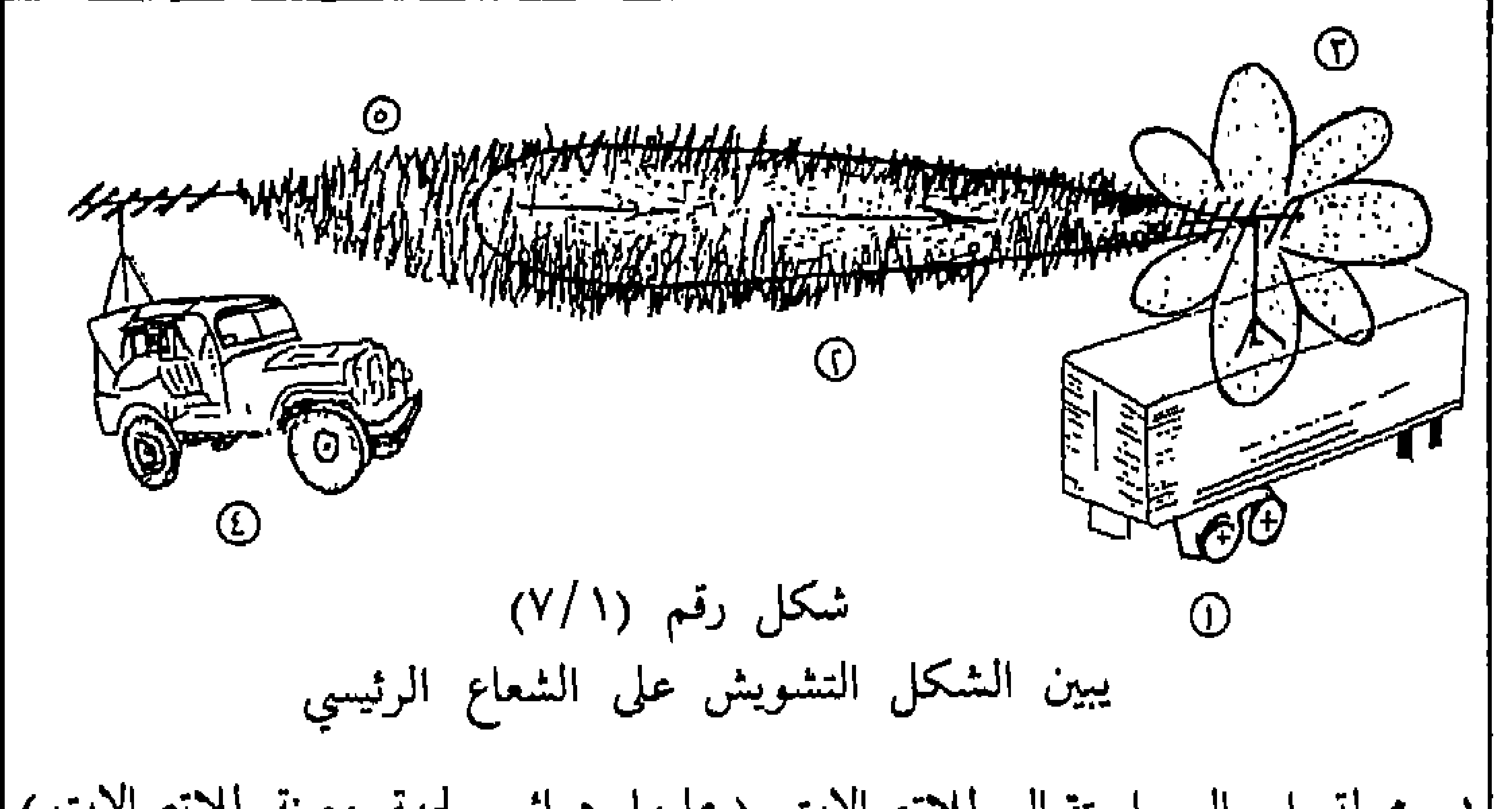
انظر شكل رقم (١/٦)، (١/٧)
وانظر شكل رقم (١/٨) و (١/٩)



شكل رقم (١/٦)

يبين الفرق بين مدى وبعد الإرسال والاستقبال لدى الهوائي لجهة واحدة بين الشعاع الرئيسي والأشعة الجانبية الأخرى.

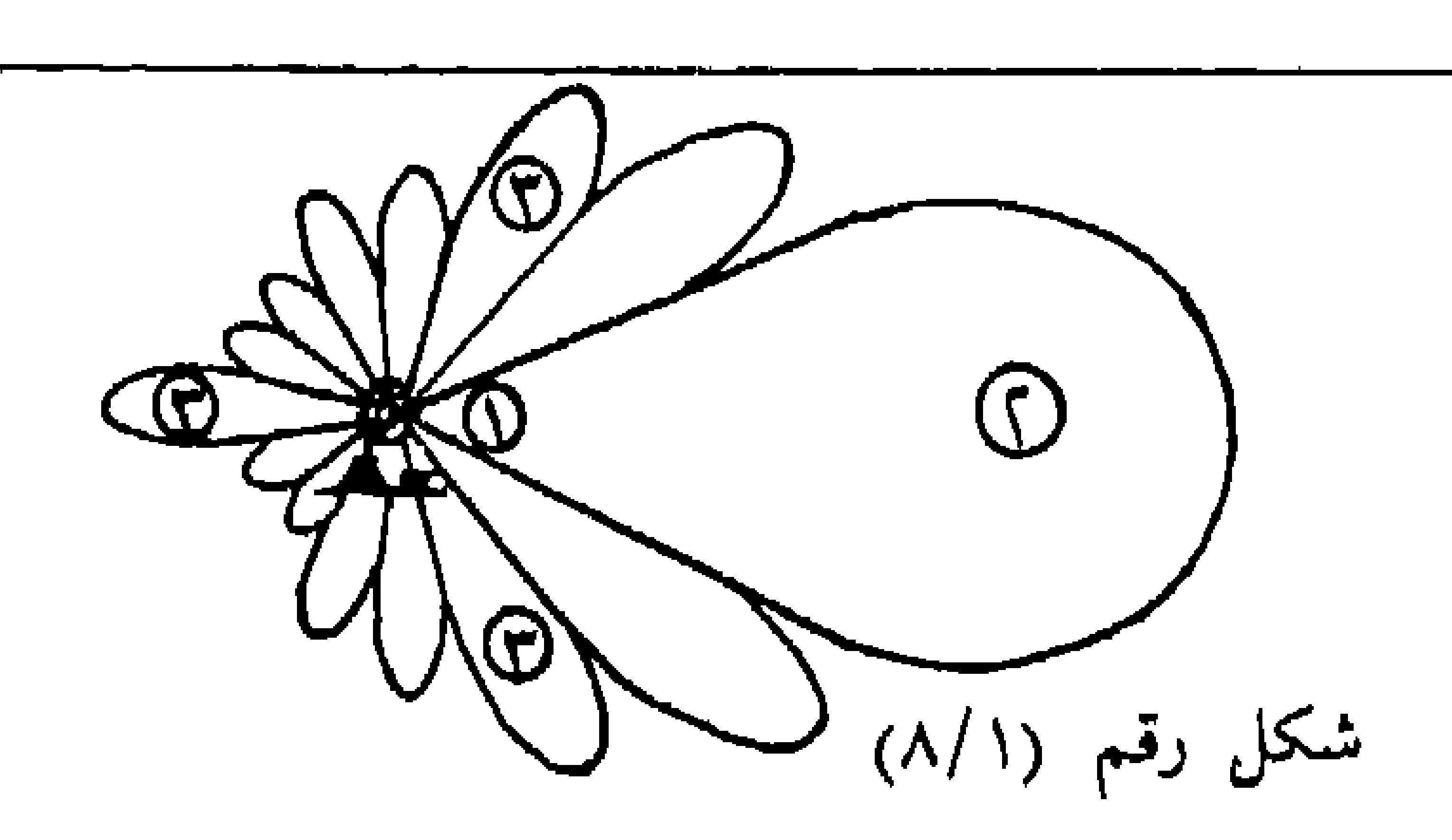
١ ـ هوائي اتصالات لجهة معينة (COMMUNICATION DIRECTIONAL ANTENNA)
٢ ـ الشعاع الرئيسي للهوائي (MAIN BEAM OR MAIN LOBE)
٣ ـ الأشعة الجانبية للهوائي (SIDE BEAMS OR SIDE LOBES)



شكل رقم (١/٧)

يبين الشكل التشويش على الشعاع الرئيسي

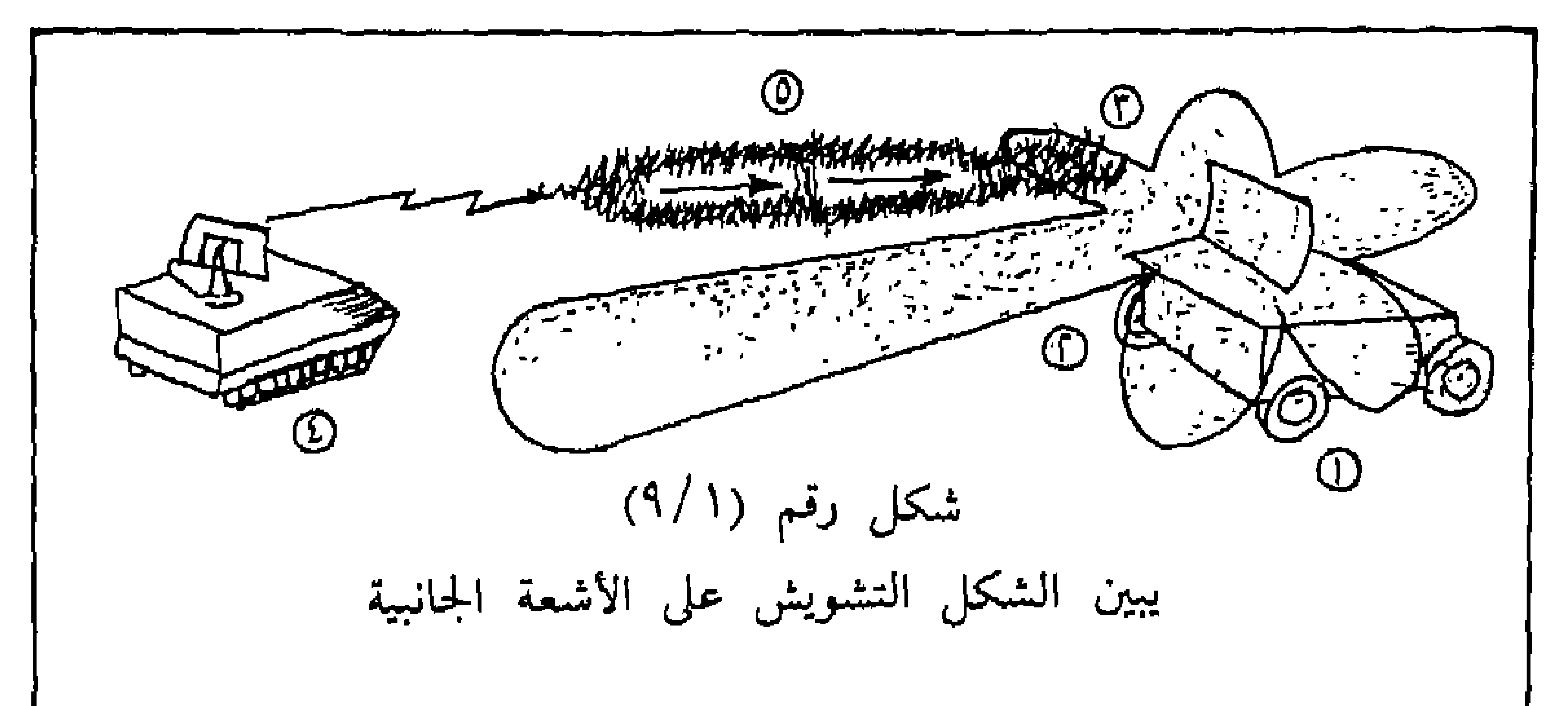
١ ـ محطة ارسال واستقبال للاتصالات (عليها هوائي لجهة معينة للاتصالات)
٢ ـ الشعاع الرئيسي (MAIN LOBE) للهوائي.
٣ ـ الأشعة الجانبية (SIDE LOBES) للهوائي.
٤ ـ جهاز تشويش للإتصالات (عليه هوائي تشويش لجهة معينة للإتصالات).
٥ ـ الشعاع الرئيسي لإشارة التشويش مسلط على الشعاع الرئيسي لمحطة الإتصالات.



شكل رقم (١/٨)

يبين الشكل: الفرق بين مدى وبعد الإرسال والإستقبال لدى الهوائي لجهة واحدة وذلك بين الشعاع الرئيسي والأشعة الجانبية الأخرى.

١ ـ هوائي رادار لجهة معينة (RADAR DIRECTIONAL ANTENNA)
٢ ـ الشعاع الرئيسي للهوائي (MAIN BEAM OR MAIN LOBE)
٣ ـ الأشعة الجانبية للهوائى (SIDE BEAMS OR SIDE LOBES)



شكل رقم (١/٩)

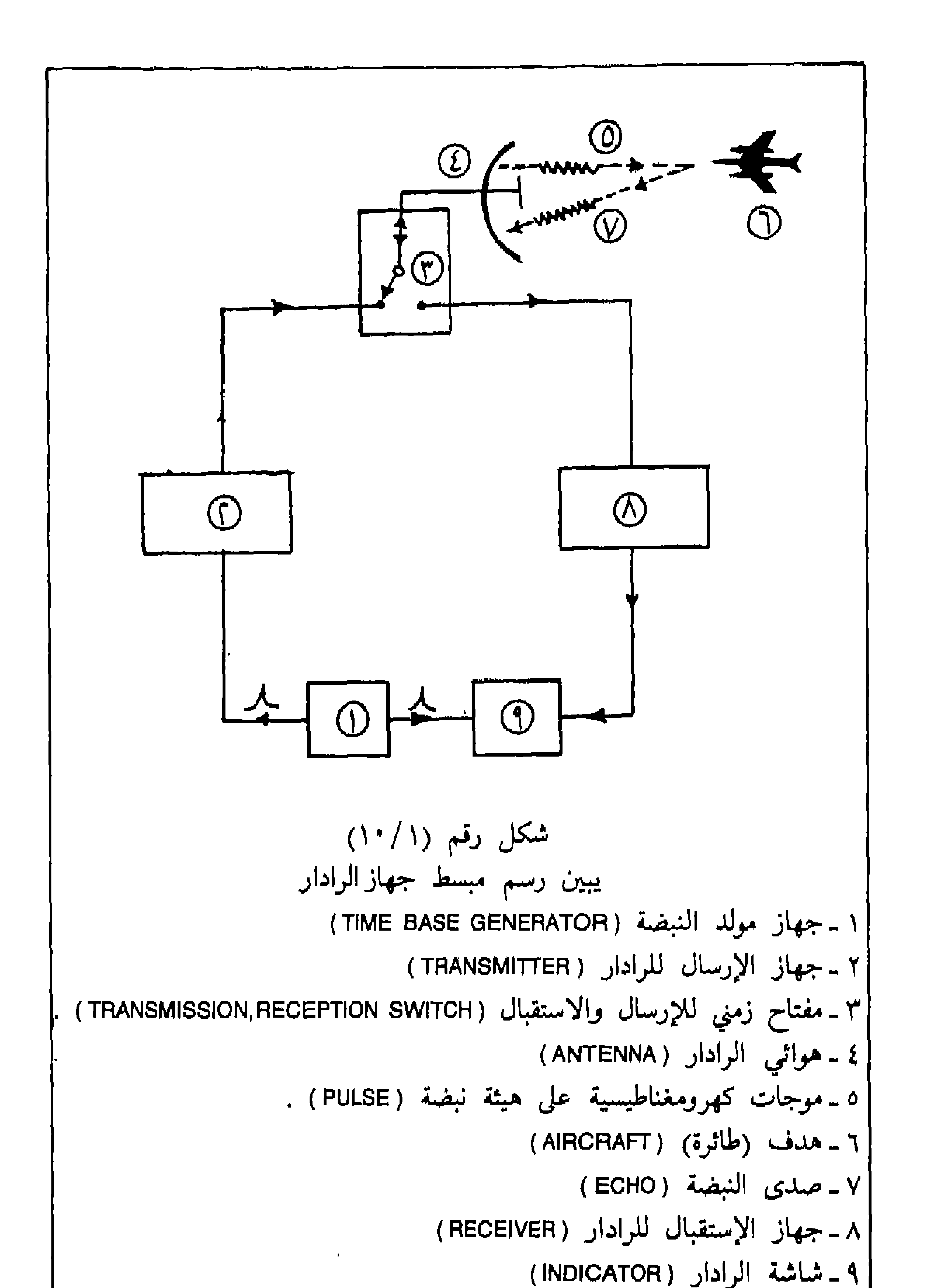
يبين الشكل التشويش على الأشعة الجانبية

١ ـ رادارا كشف (إرسال واستقبال).
٢ ـ الشعاع الرئيسي لرادار الكشف.
٣ ـ الأشعة الجانبية لرادار الكشف.
٤ ـ رادار التشويش.
٥ ـ إشارة التشويش لرادار التشويش مسلطة على الأشعة الجانبية لرادار الكشف.

ثانياً : الرادار ((RADAR) :

ويعني الرادار هو إستخدام الراديو للكشف ومعرفة بُعد الأهداف. RADAR) RADIO DETECTION AND RANGING) كذلك بدأت فكرة الرادار لجعل الإنسان يعلم عن الأشياء (أو الأهداف) التي هي بعيدة عن مرمى بصره (مستفيدا من طريقة الخفاش) وذلك بإرسال نبضة كهرومغناطيسية إلى الهدف البعيد فتصدمه فترجع فيحسب بعد ومدى الهدف.

نرى هنا (انظر شكل رقم ١/١٠) أن جهاز مولد النبضة TIME BASE) GENERATOR) يرسل نبضة (PULSE) إلى شاشة الرادار (INDICATOR) للمقارنة كما سنعرف ـ ونبضة أخرى نفس الحجم والوقت إلى جهاز الإرسال الذي يرسلها عبر هوائي الرادار عن طريق مفتاح زمني لإرسال واستقبال النبضة TRANSMISSION, RECEPTION SWITCH) وعند استقبال النبضة بعد اصطدامها بالهدف وتسمى الصدى (ECHO) ترسل للمستقبل ثم إلى شاشة الرادار ثم يحسب وقت الذهاب والإياب لمعرفة بعد الهدف.



شكل رقم (١/١٠)
يبين رسم مبسط جهاز الرادار

١ ـ جهاز مولد النبضة (TIME BASE GENERATOR)
٢ ـ جهاز الإرسال للرادار (TRANSMITTER)
٣ ـ مفتاح زمني للإرسال والاستقبال (TRANSMISSION, RECEPTION SWITCH).
٤ ـ هوائي الرادار (ANTENNA)
٥ ـ موجات كهرومغناطيسية على هيئة نبضة (PULSE).
٦ ـ هدف (طائرة) (AIRCRAFT)
٧ ـ صدى النبضة (ECHO)
٨ ـ جهاز الإستقبال للرادار (RECEIVER)
٩ ـ شاشة الرادار (INDICATOR)

وبما أن جميع هوائيات الرادارات تعتبر ذات إتجاه واحد (DIRECTIONAL ANTENNA) فهي تدور ٣٦٠° درجة للكشف عن الأهداف في جميع الاتجاهات فحالما يلتقط الصدى تحدد كذلك شاشة الرادار إتجاه الهدف.

في شرحنا لأسس الحرب الإلكترونية سنتطرق كثيراً إلى ذكر نظم أو أجهزة إيجابية أو سلبية.

١ ـ الأيجابي (ACTIVE)

وهي تعني أن الأجهزة لها خاصية الإرسال والإستقبال. (TRANSMITTING, AND RECEIVING) فيكون إرسالها عرضة للالتقاط والرصد لمعرفة المعلومات المرسلة وتحديد مكان جهاز الإرسال .

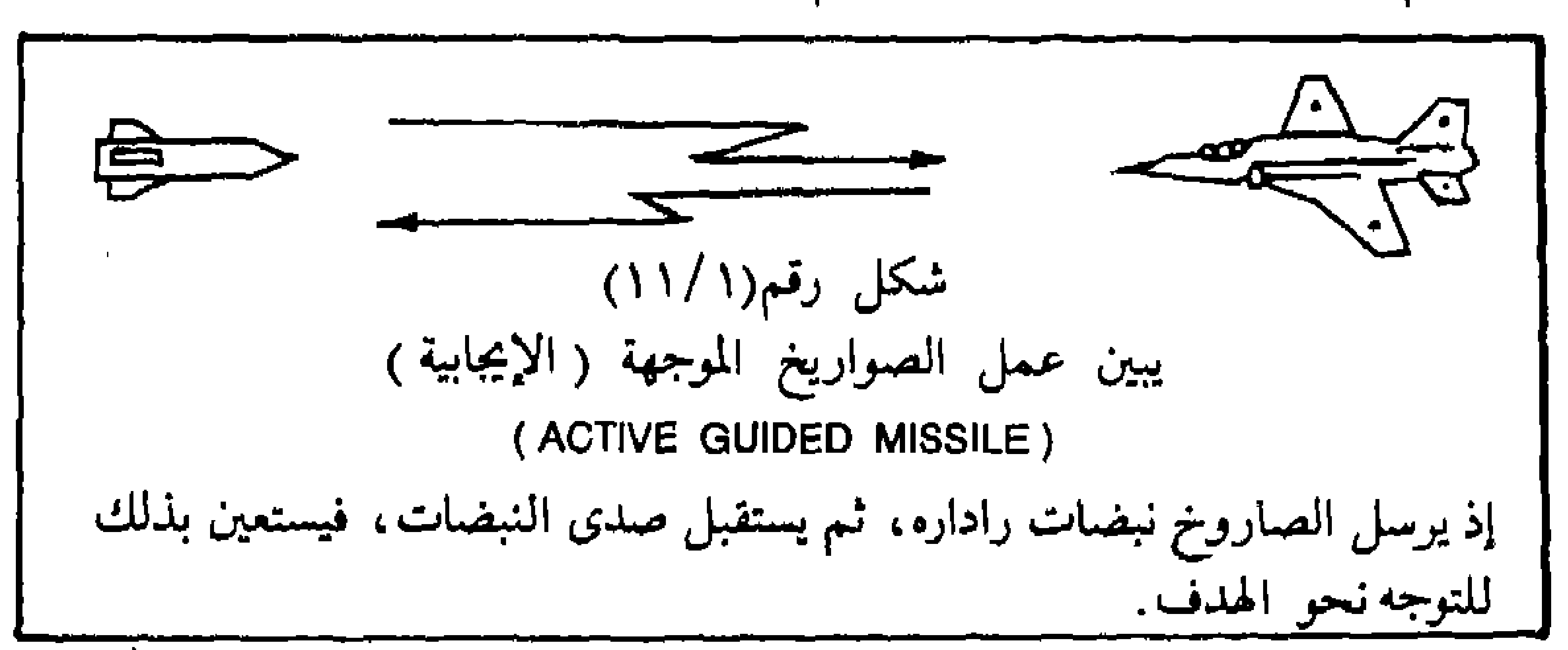
٢ ـ السلبي (PASSIVE) :

وهي تعني أن الأجهزة لها خاصية الاستقبال (RECEIVING) فقط، فتكون بذلك أقل عرضة لتحديد مكانها.

وسنستعين بالصواريخ الموجهة (GUIDED MISSILE) كمثال لادراك معنى الأجهزة الإيجابية والسلبية وما بينها.

أ ـ الصواريخ الموجهة الإيجابية (ACTIVE GUIDED MISSILE)

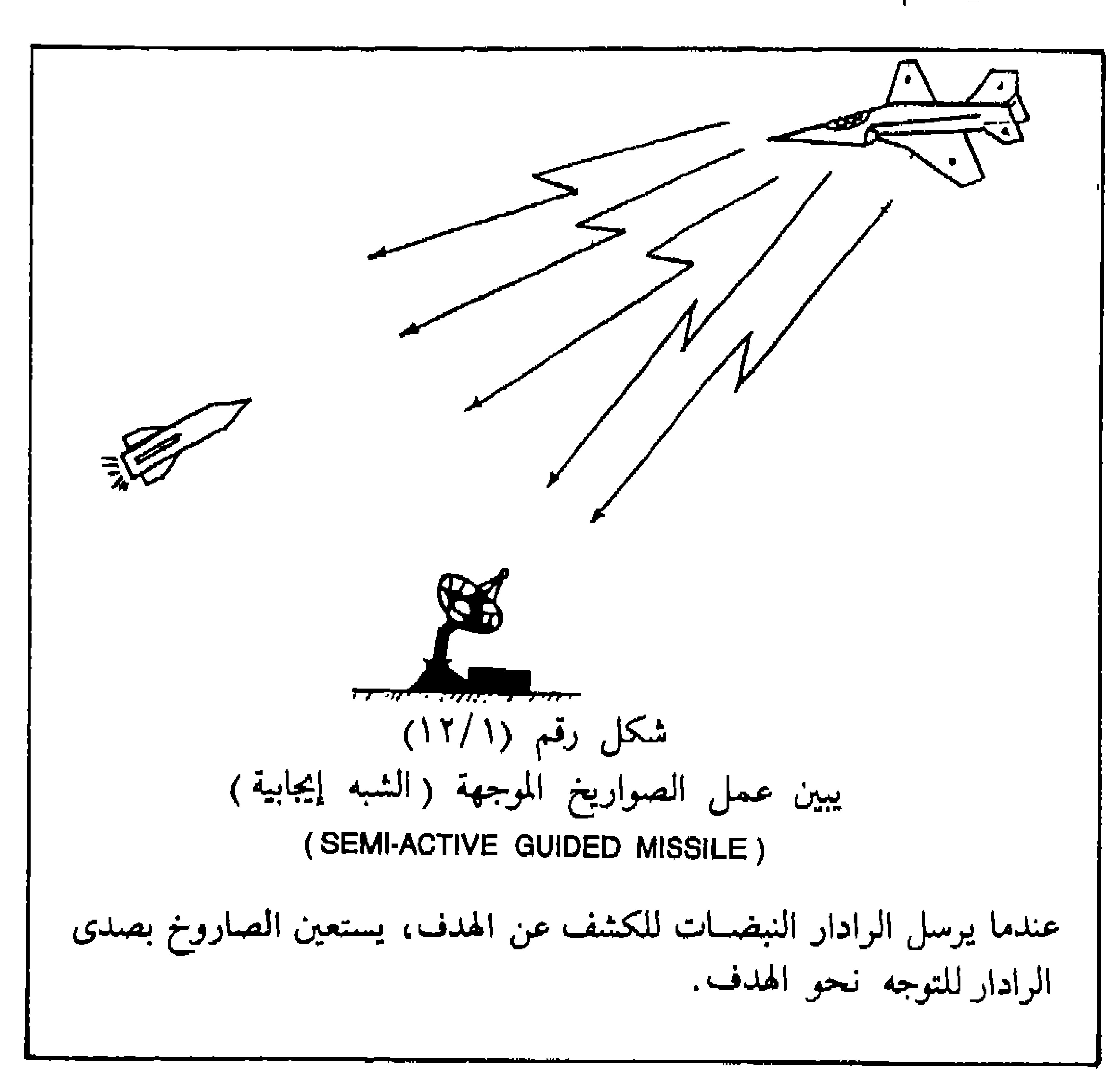
وهي التي بها جهاز رادار إرسال واستقبال لتحديد مكان واتجاه وسرعة وارتفاع الهدف ومن ثم التوجه إليه. انظر شكل رقم (١/١١).



شكل رقم(١/١١)
يبين عمل الصواريخ الموجهة (الإيجابية)
(ACTIVE GUIDED MISSILE)
إذ يرسل الصاروخ نبضات راداره، ثم يستقبل صدى النبضات، فيستعين بذلك للتوجه نحو الهدف.

ب ـ الصواريخ الموجهة الشبه إيجابية (SEMI-ACTIVE GUIDED MISSILE)

وهي التي بها جهاز رادار استقبال فقط، الذي يستقبل صدى ارسال الرادار الأرضي الصديق ويستعين بذلك الصدى لتحديد مكان الطائرة المعادية والتوجه نحوها. انظر شكل رقم (١٢/١).



شكل رقم (١٢/١)

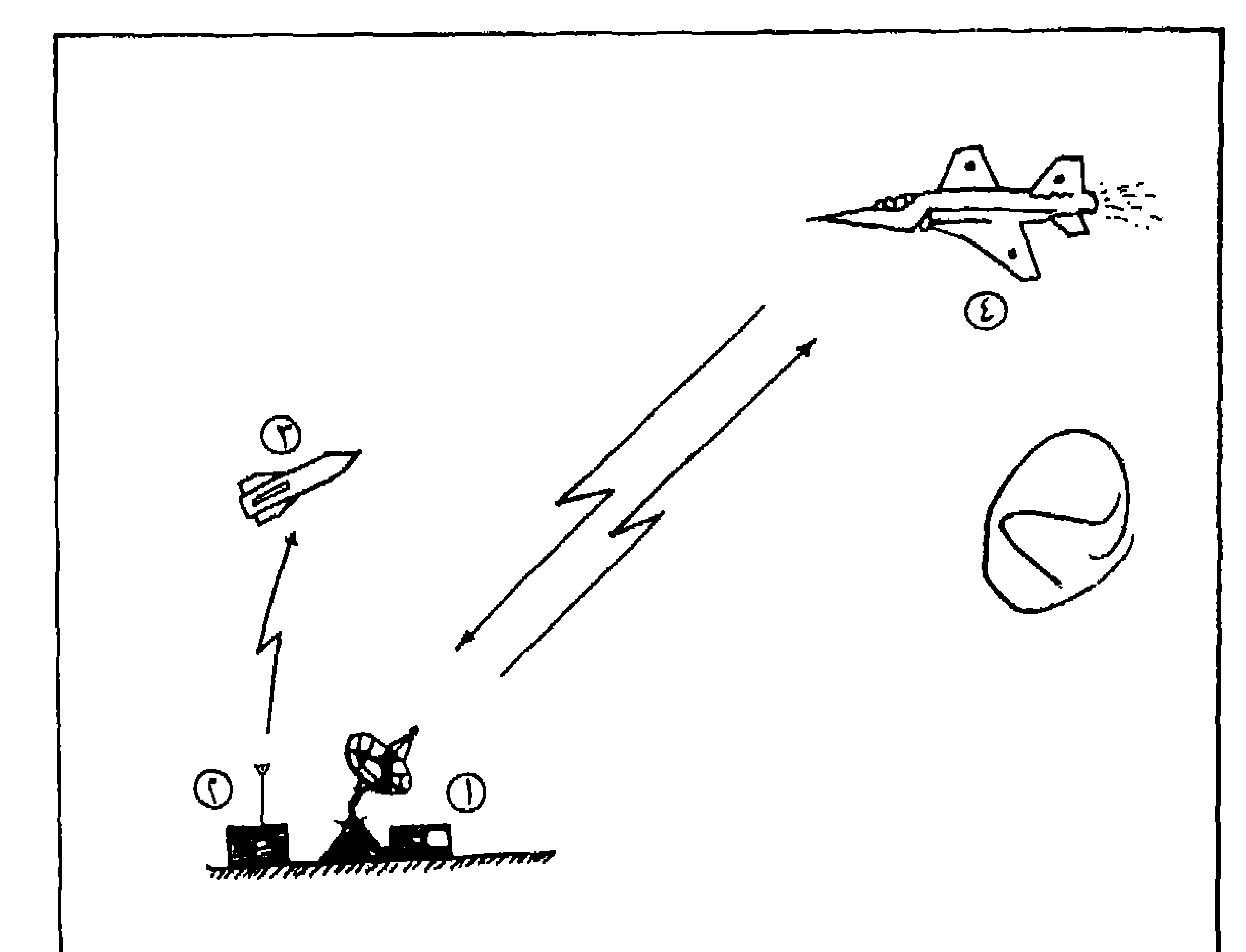
يبين عمل الصواريخ الموجهة (الشبه إيجابية)

(SEMI-ACTIVE GUIDED MISSILE)

عندما يرسل الرادار النبضـات للكشف عن الهدف، يستعين الصاروخ بصدى الرادار للتوجه نحو الهدف.

جـ ـ الصواريخ الموجهة المستقبلة معلومات التوجيه :
(COMMAND GUIDANCE OR RETRANSMISSION GUIDED MISSILE)

وهي التي بها جهاز استقبال يستقبل فقط معلومات التوجيه من المحطة الصديقة للتوجه نحو الطائرة المعادية. انظر شكل رقم (١٣/١).



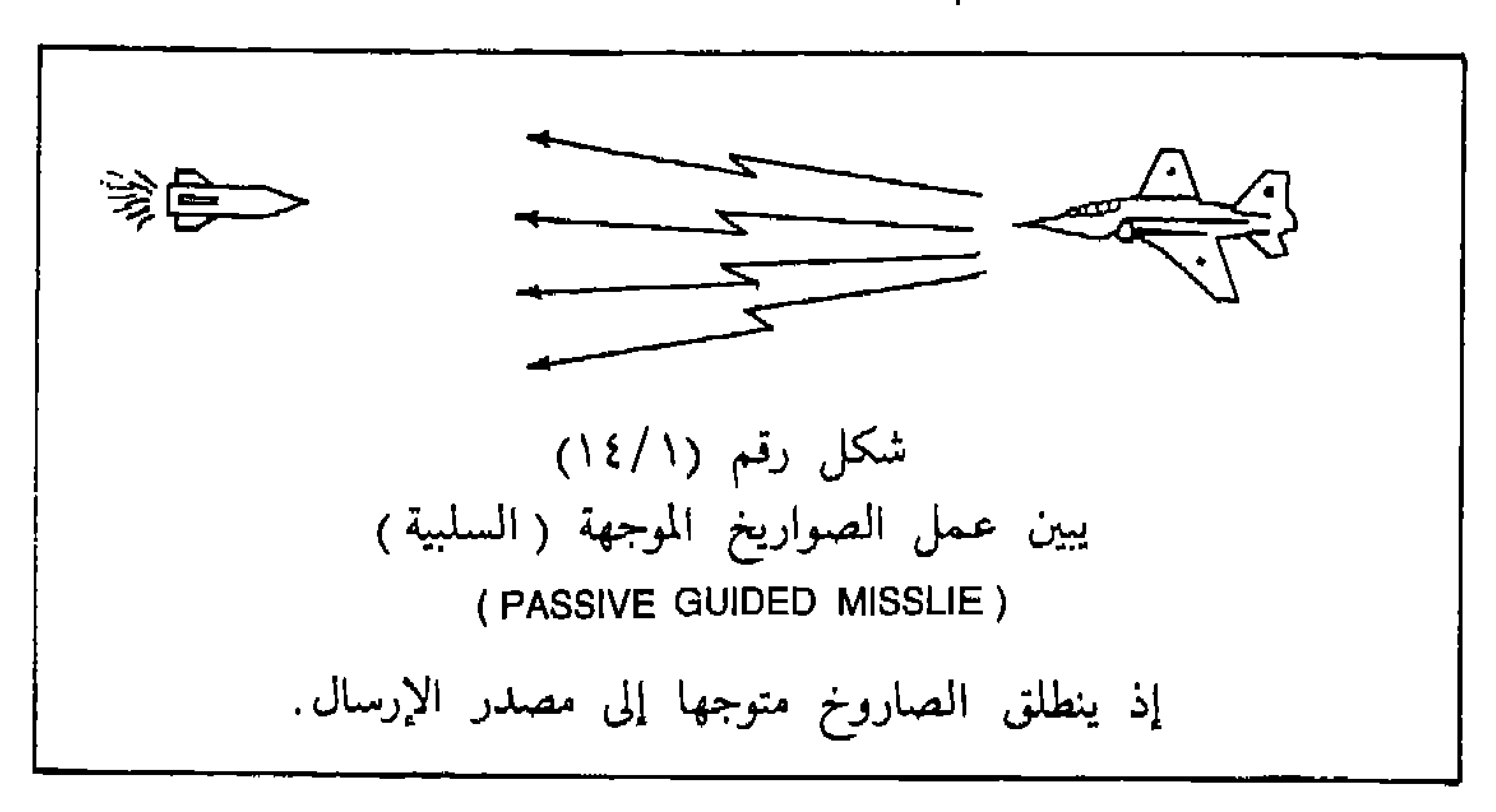
شكل رقم (١/١٣)
يبين عمل الصواريخ الموجهة المستقبلة معلومات التوجيه
(RETRANSMISSION GUIDED MISSILE OR COMMAND GUIDANCE)

١ ـ رادار كشف.
٢ ـ جهاز إرسال.
٣ ـ الصاروخ.
٤ ـ هدف.

عندما يكتشف الرادار الهدف يقوم بإرسال المعلومات إلى جهاز الإرسال ليرسلها إلى الصاروخ ليتوجه إلى الهدف.

د ـ الصواريخ الموجهة السلبية (PASSIVE GUIDED MISSILE)

وهي التي بهـا جهاز استقبـال فقط يستقبل إرسـال الطائـرة المعاديـة فيستعـين بـه للتوجه نحوها. انظر شكل رقم (١/١٤).



شكل رقم (١/١٤)
يبين عمل الصواريخ الموجهة (السلبية)
(PASSIVE GUIDED MISSLIE)
إذ ينطلق الصاروخ متوجها إلى مصدر الإرسال.

ثالثاً : الذبذبات :

الذبذبة أو التردد (FREQUENCY) تعني هنا :

هي عدد الموجات الكهربائية الكاملة في الثانية الواحدة، ووحدة قياس الذبذبة هي الهيرتز (HERTZ). .

فمثلا: ٢٥ هيرتز تعني ٢٥ موجة كهربائية كاملة في الثانية الواحدة والكيلو هيرتز (KILO HERTZ) تعادل ألف موجة كاملة في الثانية والميغا هرتز (MEGA HERTZ) تعادل مليون موجة كاملة في الثانية والقيقاهرتز (GEGA HERTZ) تعادل ألف مليون موجة كاملة في الثانية وهكذا . .

إن حاستي السمع والنظر للإنسان مرتبطة بالذبذبات فالإنسان يسمع الـذبذبـات التي من ٢٠ هرتز إلى ٢٠ ألف (كيلو) هرتز تقريبا ويستجيب لها كذلك فإن قدرته على الكلام (صوته) فهي أيضا في نفس المجال من ٢٠ هرتز إلى ٢٠,٠٠٠ هرتز تقريبا وكلما تكلم الإنسان بحدة كلما كان يستخدم الجزء الأعلى من ذلك المجال فالمرأة على

سبيل المثال عادة يكون صوتها أكثر حدة من كلام الرجل فهي إذاً تستخدم المجال الأعلى من ذلك المجال وهكذا . . .

كذلك فعين الإنسان تبصر فقط الأجسام التي تشع ضوءا كالشمس مثلا أو تعكس الضوء كالقمر مثلا، فبصر الإنسان لا يرى إلا الضوء الذي في مجال: من ٤٢٠×١٠^١٢ هرتز إلى ٧٥٠×١٠^١٢ هرتز تقريبا، وتتكون لديه الصورة التي هي مجموعة ذبذبات في ذلك المجال ليرى الأشياء وألوانها إذ لكل لون مجال ذبذبات خاصة به في نفس مجال الضوء المذكور.

لكن الإنسان يرى فقط الأشياء التي عند مد بصره فإذا كانت الأشياء أبعد من ذلك لا يراها أو كذلك إذا كان الصوت الذي يريد سماعه أبعد من مدى سمعه فيحتاج إلى أجهزة إلكترونية مثلا لتعينه على ذلك وهي فكرة التلفزيون لنقل الصورة البعيدة عن مرمى بصره والراديو لنقل الصوت البعيد عن سمعه.

ينقسم مجال الذبذبات أو الترددات العامة (FREQUENCY SPECTRUM) إلى المجالات التالية ولكل مجال إستخدامه الخاص. وسنذكر بعض الإستخدامات العسكرية في كل مجال:

أ ــ ذبذبات متدنية جدا (VERY LOW FREQUENCY) وهي من ٣ كيلو هرتز إلى ٣٠ كيلو هرتز وهي لإتصالات الغواصات.

ب ــ ذبذبات متدنية (LOW FREQUENCY) وهي من ٣٠ كيلو هرتز إلى ٣٠٠ كيلو هرتز وهي كذلك لإتصالات الغواصات والأجهزة الملاحية.

جـ ــ ذبذبات متوسطة (MEDIUM FREQUENCY) وهي من ٣٠٠ كيلو هرتز إلى ٣ ميغا هرتز وهي للإتصالات البعيدة المدى والأجهزة الملاحية.

د ــ ذبذبات عالية (HIGH FREQUENCY) وهي من ٣ ميغا هرتز إلى ٣٠ ميغا هرتز وهي للإتصالات البعيدة وللسفن الحربية وبعض الرادارات التي تكشف عبر الأفق والأجهزة الملاحية.

هـ ــ ذبذبات عالية جدا (VERY HIGH FREQUENCY) وهي من ٣٠ ميغا هرتز إلى ٣٠٠ ميغا هرتز لإتصالات السفن والطائرات الحربية وإتصالات القوات البرية والأجهزة الملاحية.

و ــ ذبذبات (ULTRA HIGH FREQUENCY) وهي من ٣٠٠ ميغا هرتز إلى ٣ قيقا هرتز

وهي لإتصالات الطائرات وللإتصالات الأرضية المتعددة القنوات وبعض الرادارات والأجهزة الملاحية.

ز ـ ذبذبات (SUPER HIGH FREQUENCY) وهي من ٣ قيقيا هرتز إلى ٣٠ قيقا هرتز وهي للرادارات وأجهزة إتصالات الميكروويف والصواريخ والأقمار الصناعية.

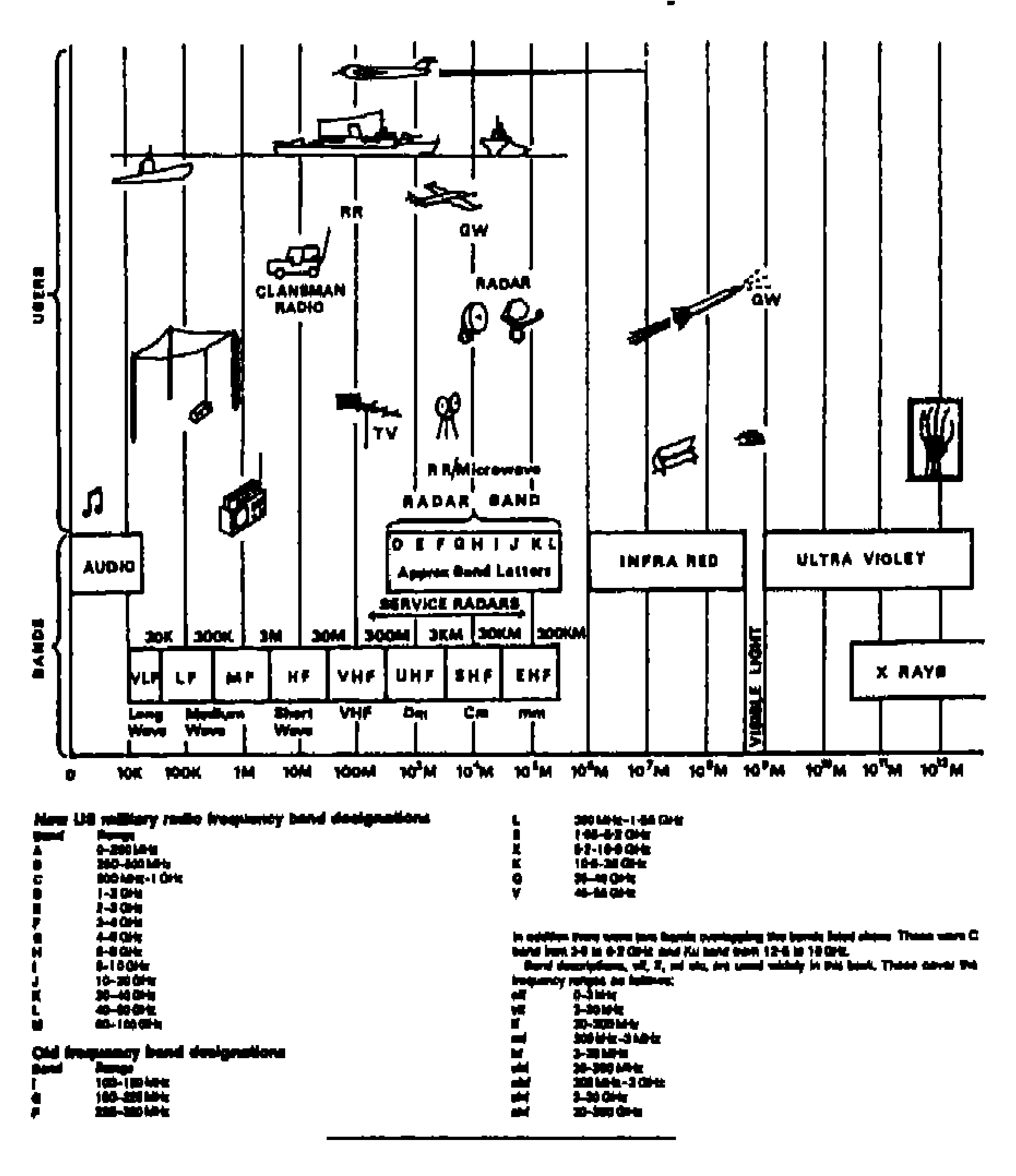
ح ـ ذبذبات (EXTEREMLY HIGH FREQUENCY) وهي من ٣٠ قيقا هرتز إلى ٣٠٠ قيقا هرتز وهي لبعض الرادارات والصواريخ، والاتصالات الأرضية التكتيكية.

وهناك تقسيم آخر لمجال الذبذبات وهو حسب تطبيقاتها:

١ ـ ذبذبات عسكرية. (MILITARY FREQUENCIES) .

٢ ـ ذبذبات مدنية. (CIVIL FREQUENCIES) .

٣ ـ ذبذبات هواة اللاسلكي (RADIO AMATEUR'S FREQUENCIES) .



٢ ـ التعريف بالحرب الإلكترونية

إن للحرب الإلكترونية تعاريف كثيرة وتختلف من كتاب لآخر وذلك لأن موضوعها موضوع شائك ومتشعب وبما أن التعريف يجب أن يكون محددا وليس هناك تعريف محدد متفق عليه دوليا، فكل جهة تعرفه بما يتناسب مع مفهومها للحرب الإلكترونية، لذا سنذكر بعض هذه التعاريف المختلفة المصادر ومن ثم سنبلورها في تعريف يكون جامعا لكل التعاريف مع شرح ذلك التعريف حتى نخرجه بصورة جيدة تعيننا في معرفة كنه موضوع الحرب الإلكترونية (وهذا ما سنفعله أيضا عندما نعرف أسس الحرب الإلكترونية) :

١ ـ تعريف حلف الناتو للحرب الإلكترونية:

ELECTRONIC WARFARE IS

" THAT DIVISION OF THE MILITARY USE OF ELECTRONICS INVOLVING ACTIONS TAKEN TO PREVENT OR REDUCE AN ENEMY'S EFFECTIVE USE OF RADIATED ELECTRO-MAGNETIC ENERGY AND ACTIONS TAKEN TO ENSURE OUR OWN EFFECTIVE USE OF RADIATED ELECTRO-MAGNETIC ENERGY ".(1)

ويترجم هذا التعريف على النحو التالي:

الحرب الإلكترونية هي « ذلك القسم العسكري الذي يستخدم إلكترونيات تهتم بالإجراءات التي تتخذ لمنع أو تقليل استخدام العدو لطاقته الكهرومغناطيسية المنبعثة الفعالة، والإجراءات التي تتخذ لحماية طاقتنا الكهرومغناطيسية المنبعثة الفعالة ».

٢ ـ تعريف الحرب الإلكترونية في كتاب: **(ELECTRONIC COUNTERMEASURES)**

الذي أصدره معهد العلوم والتكنولوجيا في جامعة مشيقن لسلاح الإشارة في القوات البرية الأمريكية.

---

(١) كتاب INTELLIGENCE WARFARE لمؤلفه: الكولونيل وليم كيندي صفحة ٧٦، صدر في عام ١٩٨٣م.

التعريف (في صحة ٢ ـ ١)

" THE EMPLOYMENT OF ELECTRONIC DEVICES AND TECHNIQUES FOR THE PURPOSES OF:

a. DETERMINING THE EXISTENCE AND DISPOSITION OF THE ENEMY'S ELECTRONIC AIDS TO WARFARE.

b. DESTROYING OR DEGRADING THE EFFECTIVENESS OF THE ENEMY'S ELECTRONIC AIDS TO WARFARE.

C. PREVENTING THE DESTRUCTION OF THE EFFECTIVENESS OF FRIENDLY ELECTRONIC AIDS.

ومعنى التعريف :

الحرب الإلكترونية هي : استخدام الأجهزة والتقنيات الإلكترونية للأغراض التالية :

أ ـ تحديد وجود المساندة الإلكترونية المعادية في العمليات الحربية.

ب ـ تدمير أو إفساد المساندة الإلكترونية الفعالة المعادية في العمليات الحربية.

جـ ـ منع تدمير المساندة الإلكترونية الفعالة الصديقة.

٣ ـ التعريف في كتاب «الحرب الإلكترونية» لكمال السعدي طبعة ١٩٧٩ صفحة٩.

«هو استخدام التقنيات الإلكترونية المعروفة على اختلاف أنماطها في مواجهة أنظمة السلاح التي يملكها الخصم».

٤ ـ التعريف في كتاب (WORLD ELECTRONIC WARFARE AIRCRAFT)

(THE USE OF ELECTRO-MAGNETIC EMISSIONS AS: A WEAPON OR INTELLIGENCE SOURCE)

ومعنى التعريف : استخدام الإنبعاثات الكهرومغناطيسية كسلاح أو مصدر للإستخبارات .

٥ ـ التعريف في كتاب (THE INTERNATIONAL COUNTERMEASURES HANDBOOK) طبعة ١٩٧٦ ـ ١٩٧٧ صفحة ٥٩٩. (وهذا التعريف هو المعتمد لدى وزارة الدفاع الأمريكية).

وهو كذلك تعريف شركة (WATKINS-JOHNSON) الأمريكية.

(MILITARY ACTION INVOLVING THE USE OF ELECTRO-MAGNETIC ENERGY TO DETERMINE, EXPLOIT, REDUCE, OR PREVENT HOSTILE USE OF THE ELECTRO-MAGNETIC SPECTRUM, AND ACTION WHICH RETAINS FRIENDLY USE OF THE ELECTRO-MAGNETIC SPECTRUM).

ومعنى التعريف كالآتي:

«الإجراء العسكري المتضمن إستخدام الطاقة الكهرومغناطيسية لتحديد أو إستغلال أو التقليل أو منع العدو من إستخدام موجاته في المجال الكهرومغناطيسي، والإجراء الذي يحمي الموجات الصديقة في المجال الكهرومغناطيسي .

والآن سنعرف الحرب الإلكترونية بمفهومنا المتواضع على ضوء قراءتنا وإدراكنا في هذا الموضوع .

فنعني بعبارة «الحرب الإلكترونية»:

«العمليات التي تستخدم فيها أساليب ومعدات إلكترونية للإستفادة من موجات العدو الكهرومغناطيسية الفعالة المنبعثة من معداته المختلفة، والتأثير على معداته لمنع أو تقليل استفادته منها، ولحماية موجاتنا الكهرومغناطيسية الفعالة المنبعثة من معداتنا المختلفة من استفادة العدو منها، أو التأثير على معداتنا».

إذن فالحرب الإلكترونية تعني هنا العمليات أو الإجراءات المتخذة أو الأوضاع أو الحالات (العسكرية عادة) التي تستخدم في أثنائها أساليب وطرق وخطوات معينة مدروسة كأن تكون عمليات الحرب الإلكترونية في أوقات معينة نهارا أو ليلا، في حالة الهجوم أو في حالة الدفاع أو أن تستخدم أرضية معينة (PLATFORM) من طائرات أو سفن أو آليات عسكرية كذلك تحديد أماكن عمليات الحرب الإلكترونية، ويكون هذا مصحوبا باستخدام معدات إلكترونية متخصصة في عمليات الحرب الإلكترونية من أجهزة استطلاع ومراقبة (أجهزة استقبال) إلكترونية متطورة وكاميرات وأجهزة كشف مختلفة، وكذلك استخدام أجهزة تشويش ومخادعة وتضليل إلكترونية لتقليل فعالية أجهزة العدو، واستخدام أجهزة متخصصة للحماية الإلكترونية مثل الهوائيات الموجهة وأجهزة التشفير . . . الخ، للحماية من المراقبة والتشويش المعادي .

والآن سنحاول بشيء من التفصيل شرح بعض الكلمات المدرجة في التعريف لكي نعطي تصورا أكبر لمفهوم الحرب الإلكترونية.

«فالعمليات» هنا كما قلنا هي الحالات أو الأعمال التنفيذية التي نقوم بها مستخدمين ـ إلكترونيا ـ أساليب محددة وأجهزة متخصصة للإستفادة والتأثير والحماية الإلكترونية.

والإستفادة : تكون باستخدام أساليب وأجهزة إلكترونية متخصصة لرصد وكشف واستطلاع ومراقبة جميع موجات العدو الكهرومغناطيسية المنبعثة من أجهزته اللاسلكية المختلفة. ثم تحليلها ومعرفة محتواها بهدف الوقوف على نوعية معداته وقواته وتحركاته وتشكيلاته وإمكاناته وخططه العسكرية، فتكون سياستنا وتعاملنا معه بعد ذلك طبقا لإجراءات وأساليب مناسبة وحكيمة.

وهذه الإستفادة «تسمى في مفهوم الحرب الإلكترونية: الإجراءات الإلكترونية المساندة: (ELECTRONIC SUPPORT MEASURES « ESM »)

والتأثير على أجهزة العدو يكون باستخدام أساليب وأجهزة الكترونية متخصصة تنبعث منها موجات كهرومغناطيسية بطاقة موجهة نحو أجهزة العدو لتعمل على تقليل أو منع العدو من الإستفادة من أجهزته الإلكترونية المختلفة (التشويش) وبالتالي ستؤثر وتعيق عملياته وسيطرته وقيادته العسكرية، وهذا «التأثير» يسمى في مفهوم الحرب الإلكترونية «الإجراءات الإلكترونية المضادة». (ELECTRONIC COUNTER MEA- SURES « ECM »)

والحماية تعني استخدام الأساليب الفنية والأجهزة الإلكترونية المتخصصة لتقليل أو منع العدو من التأثير (أو التشويش) على أجهزتنا الإلكترونية المختلفة وكذلك تقليل أو منع العدو من الإستفادة من الموجات الكهرومغناطيسية المنبعثة من أجهزتنا الإلكترونية المختلفة.

ولاشك أننا إذا نجحنا وأحكمنا هذه الحماية ستكون عملياتنا وسيطرتنا وقيادتنا على أسلحتنا ومعداتنا موفقة.

وهذه «الحماية» تسمى في مفهوم الحرب الإلكترونية: المضادات الإلكترونية للإجراءات المضادة (ELECTRONIC COUNTER-COUNTER MEASURES « ECCM ») وكذلك تسمى : إجـراءات الحمايـة الإلكترونيـة (ELECTRONIC PROTECTIVE MEA- SURES "E.P.M") **ويجب أن نعلم أن عمليات الاستفادة والتأثير والحماية قد تحدث في** حالة السلم كما تحدث في حالة الحرب، وكما أنها تحدث في النشاطات العسكرية فيمكن أن

تحدث في النشاطات المدنية مثل أقسام وأجهزة الحكومة الرسمية .

كما أننا نلفت الإنتباه إلى أن تلك الموجات المنبعثة من الأجهزة الإلكترونية تكون عادة على شكل إنبعاثات كهرومغناطيسية (ELECTRO-MAGNATIC EMISSIONS) ذات طاقة (ENERGY) وتستخدم هذه الموجات حيزا معينا من المجال أو الطيف المعروف وهو من ٣ كيلو هرتز إلى بلايين من الهرتز (انظر شكل(١/١٥))،حيث تنبعث من هوائيات (ANTENNAS) الأجهزة الإلكترونية وتنتشر وترسل عبر الأثير (مثل إرسال أجهزة الإتصالات والرادار والأجهزة الملاحية . . الخ) .

وبما أن الإستفادة الإلكترونية (ESM) والتأثير الإلكتروني (ECM) والحماية الإلكترونية (ECCM) معظمها ناتجة عن الإنبعاثات الكهرومغناطيسية ، لذا فإنه يطلق على الحرب الإلكترونية في بعض الكتب تعبير: (الحرب الكهرومغناطيسية) (ELECRTO-MAGNATIC WARFARE) وهي تحوي كل نظم وطاقات الموجات الكهرومغناطيسية من أجهزة الإرسال والإستقبال الراديوية ، الـرادار، الأجهزة الملاحية وأجهزة الليزر. . الخ .

وقد قال الأدميرال توماس هـ. مورو الذي شغل منصب رئيس المجلس المشترك لرؤساء الأركان الأمريكية في الفترة من ١٩٧٠ إلى ١٩٧٤م أنه : إذا حدثت الحرب العالمية الثالثة : فسيكون النصر للجانب الذي يتحكم في المجال الكهرومغناطيسي[١] .

وإذا رجعنا إلى التعريف فإننا نجد كلمة (**الفعالة**) في (الموجات الكهرومغناطيسية الفعالة) وتعني : الموجات التي تحوي معلومات إذا ما حللت وفندت نستطيع أن نحصل على خواص الأجهزة والمعدات والأنظمة والأسلحة المنبعثة منها، كما نستطيع معرفة بعض المعلومات القيمة وأسرار الجهة التي تنبعث منها تلك الموجات الكهرومغناطيسية الفعالة .

وهذه الأساليب والأجهزة الإلكترونية المستخدمة في الحرب الإلكترونية تكون مختلفة نسبياً فيها بين القوات الجوية والبرية والبحرية .

ولاشك أنك سترى الكثير من التعاريف لهذا الموضوع في الكتب والمجلات والمنشورات المتخصصة ولكن هذا هو التعريف الذي حاولنا بقدر الإمكان أن يكون

(١) مجلة MILITARY TECHNOLOGY عدد يونيو عام ١٩٨٣ صفحة ٨٢.

شاملاً لمعنى الحرب الإلكترونية. كما أنك سترى أن كل المصطلحات التي سترد فيما بعد لها تعاريف مختلفة ولكنها جميعا تنتهي إلى معنى واحد.

ولا يزال موضوع الحرب الإلكترونية غير مستوف حقه من إهتمام قادة الجيوش في معظم بلدان العالم وخاصة الدول النامية. وهناك أسباب عديدة لعدم الإهتمام بهذا الموضوع منها:

١ ــ تعتبر الدول المتقدمة هذا الموضوع من الموضوعات الحساسة لما يحويه من أسرار وخفايا الأجهزة الإلكترونية. لذا تراهم يتحاشون إعطاء ضباط الدول النامية دورات متخصصة حول هذا الموضوع. كما أن الكتب المتخصصة في موضوع الحرب الإلكترونية تتسم بالندرة.

٢ ــ تكلف أجهزة الحرب الإلكترونية (من ترصد ومراقبة وتشويش وخداع إليكتروني وكشف واستطلاع) أموالا باهظة. كما أن الشركات أو الدول المنتجة لها تفرض عند بيعها قيودا أو شروطا صارمة، حتى أنهم أحيانا يعتذرون عن بيعها.

٣ ــ جهل بعض القادة بأساسيات هذا الموضوع. واعتماد معظمهم على الأسلحة التقليدية (CONVENTIONAL WEAPONS) من قنابل ومدافع وقذائف صاروخية أو الإعتماد على الطائرات والصواريخ الموجهة (GUIDED MISSILES)، واعتبار موضوع الحرب الإلكترونية موضوعاً ثانوياً.

لكن في السنوات الأخيرة ظهرت أهمية وخطورة الحرب الإلكترونية أمام الدول النامية حين استخدمت معدات الحرب الإلكترونية في الحروب الأخيرة.

وقد بلغ من اهتمام الدول المتقدمة بموضوع الحرب الإلكترونية أن بعضها (كالولايات المتحدة الأمريكية) تدفع مبالغ هائلة للشركات الأمريكية الإلكترونية الكبرى تصل إلى بلايين الدولارات للإبتكار واختراع أجهزة جديدة ومتطورة في الحرب الإلكترونية لتزود بها القوات الأمريكية، كما أنهم يعطونهم وقتاً كافياً قد يصل إلى عشر سنوات أو أكثر للإختراع والإبتكار بعدها تحدد القوات أفضل الأجهزة وأصلحها(١).

وقد بلغت ميزانيات الإبتكار والإختراع للقوات الأمريكية في سنة ١٩٨١ حوالي

(١) مجلة JANE'S DEFENCE WEEKLY عدد ١٩٨٤/٨/١١، صفحة ١٨٠.

١,٧ بليون دولار في حين بلغت مصاريف شراء أجهزة الحرب الإلكترونية للقوات الأمريكية في نفس السنة ٢,٦ بليون دولار، ووصلت ميزانيات الحرب الإلكترونية في جميع دول العالم خلال عام ١٩٨٥ حوالي ٧,١٤ بليون دولار[١]، يكون منها حوالي ٥,٨ بليون دولار ميزانية الولايات المتحدة الأمريكية للحرب الإلكترونية.

ولكن نتبين أهمية الحرب الإلكترونية وخطورتها في عالم اليوم سنذكر على سبيل المثال لا الحصر أمثلة عن ممارستها في الحروب الحديثة.

١ ـ في حرب ١٩٧٣ حدثت معركة بين القوات السورية والقوات الإسرائيلية فقد هاجم ١١ قاربا سوريا مزودة بصواريخ روسية من نوع (STYX) مداها ٢٥ ميلاً، هاجمت ٤ قوارب إسرائيلية مزودة بصواريخ إسرائيلية الصنع نوع (GABRIEL) مداها ١٥ ميلا، وحين كان السوريون يطلقون صواريخ (STYX) كان الإسرائيليون يطلقون النصلات (CHAFF) بعيدة المدى فيتبعها الصاروخ وينحرف عن مساره، وكانت هناك بعض الصواريخ لا تتبع النصلات فيطلق الإسرائيليون نوافذ أخرى قصيرة المدى كمحاولة أخرى لإبعاد الصواريخ عن مسارها المؤدي إلى القوارب الإسرائيلية فإذا أخطأتها النصلات الأولى لحقت بالنصلات الثانية وطبعا لابد أن تكون هذه العملية سريعة جدا إذ أن وقتها لا يتعدى الثواني المعدودة وهناك أنواع من النصلات تنطلق أتوماتيكيا عند اكتشاف الرادار صواريخ موجهة، وباستخدام النصلات على هذا النحو استطاع الإسرائيليون التخلص من ٥٠ صاروخا سوريا أطلقته القوات السورية ولم تدمر أيا من القوارب الإسرائيلية وفي هذه الأثناء والعملية جارية اقتربت القوارب السورية والإسرائيلية من بعضها البعض وتمكن الإسرائيليون باستخدام صواريخهم (GABRIEL) من إغراق معظم القوارب السورية[٢].

هذا علما بأن تلك النوعية من الصواريخ الروسية (STYX) قد استخدمتها القوات البحرية المصرية في عام ١٩٦٧، عندما أطلقتها على المدمرة إيلات الإسرائيلية ودمرتها.

وكذلك استخدمتها الهند في حربها ضد باكستان في عام ١٩٧١، إذ أطلقت

---

(١) انظر THE INTERNATIONAL COUNTERMEASURES HANDBOOK ١٩٨١ - ١٩٨٢ ص٤٢.

(٢) مجلة INTERNATIONAL DEFENCE REVIEW عدد خاص عن ELECTRONIC WARFARE ١٩٧٨/٥م صفحة ٩٠.

القوات البحرية الهندية في معركة بحرية واحدة ١٣ صاروخاً من ذلك النوع أصابت منها ١٢ صاروخ بعض القطع البحرية الباكستانية.

٢ ـ في يونيو عام١٩٨٢ استطاع الإسرائيليون تحطيم حوالي مائة طائرة مقاتلة سورية و١٧ بطارية سام ٦ في وادي البقاع اللبناني خلال يومين اثنين، وقد ساعدهم على ذلك بشكل أساسي التشويش الدقيق المركز على جميع الإتصالات والرادارات والطائرات الحربية والسورية في تلك المنطقة[١].

وقد تناقلت هذا الخبر الكثير من وكالات الأنباء العالمية.

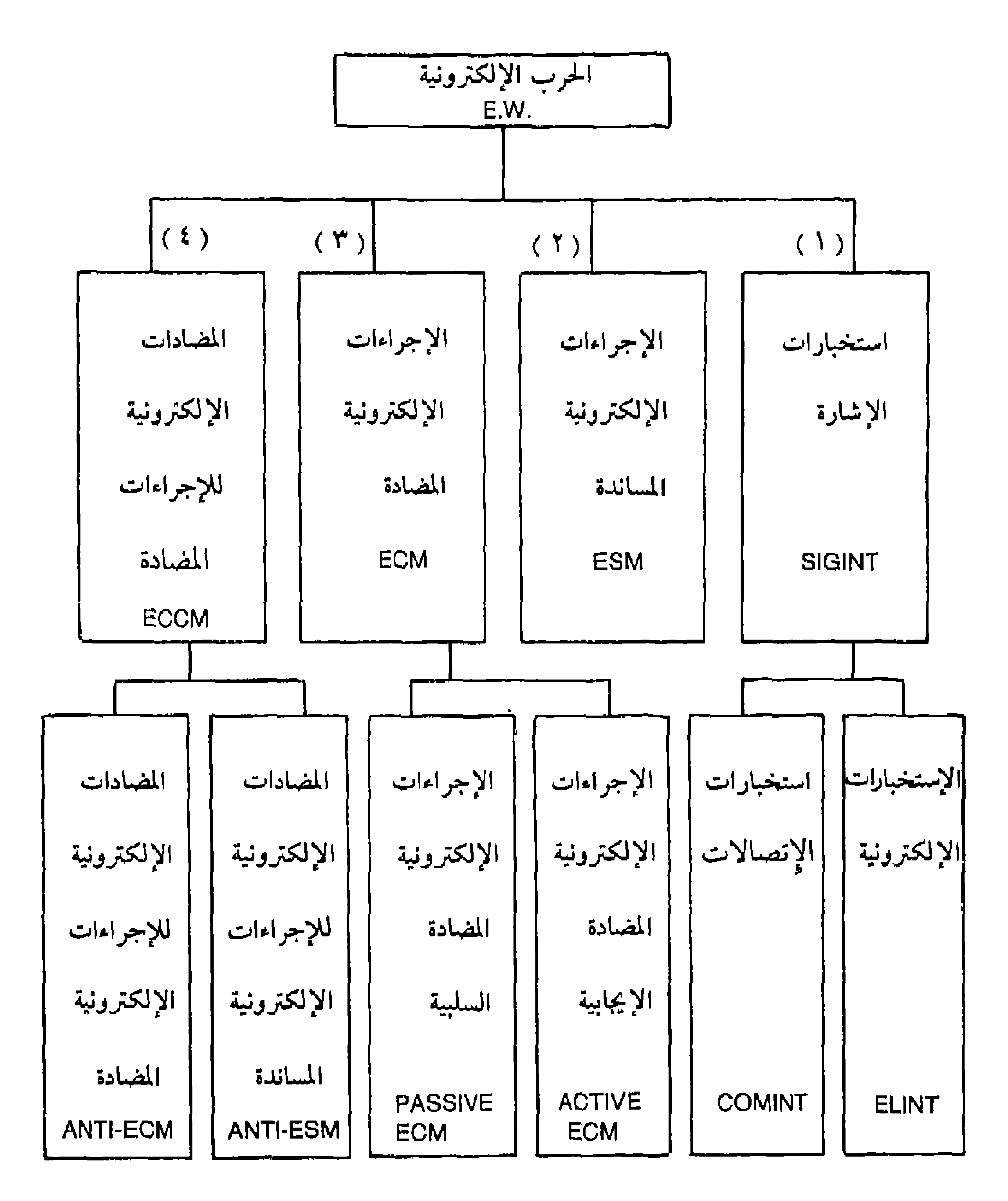
٣ ـ نقلت وكالة الأنباء الكويتية «كونا» هذا الخبر:
عندما أراد الفرنسيون في نوفمبر ٨٣ قصف التجمعات الإيرانية قرب بعلبك في لبنان أقلعت أربع طائرات قاذفة قنابل فرنسية تحميها عشر طائرات محملة فقط بأجهزة حرب إلكترونية (EW A/C) لتعطيل الأجهزة الأرضية وبالذات رادارات وصواريخ سام ٦ السورية الموجودة في تلك المنطقة، وأثناء تلك العملية أطلقت عدة صواريخ سام ٦ نحو الطائرات الفرنسية ولكن الطائرات الإلكترونية الفرنسية استطاعت بالتشويش والخداع الإلكتروني أن تعيق عمل تلك الصواريخ وتم القصف وعادت كل الطائرات الفرنسية إلى قواعدها بسلام».

٤ ـ في أواسط عام ١٩٨٣ عارض وزير الدفاع الأمريكي كاسبر واينبرغر زيادة المساعدات الأمريكية لإسرائيل وناشد الكونغرس الأمريكي خفض المساعدات وكان سبب إعتراضه الرئيسي هو أن إسرائيل لا تزود أمريكا بأسرار المعدات الروسية التي يملكها الجيش السوري وقد استعملتها سوريا ضد إسرائيل عندما غزت إسرائيل لبنان عام ١٩٨٢ فقد رصدت إسرائيل تلك المعدات وكشفت عن خواصها الفنية واستطاعت بالتالي أن تشوش عليها وتخدعها إلكترونيا وقد نجحت في ذلك.

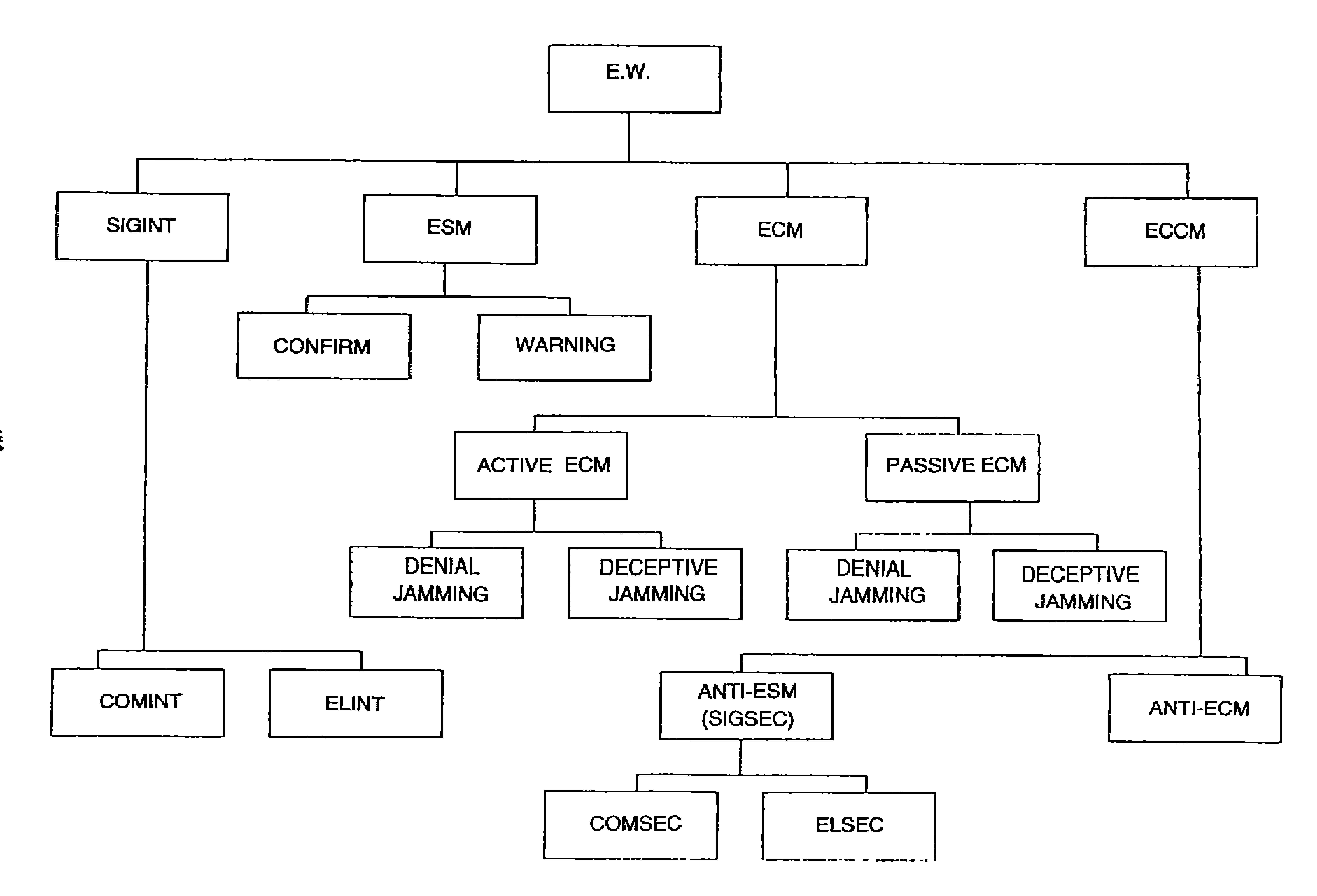
وللحرب الإلكترونية أسس يوضحها الشكلين التاليين :

---

(١) انظر الباب الرابع.



وهذا النموذج ما هو إلا توضيح مبسط لأسس الحرب الإلكترونية وإذا ما فهمنا هذه الأسس نستطيع ببساطة أن نعرف أو على الأقل نقدر ماذا يدور حولنا ونفسر ما تتناقله الصحف والمجلات والكتب والتقارير عن الحروب والمعارك البحرية والبرية والجوية المتضمنة عمليات حرب إلكترونية.


E.W.
SIGINT
ESM
ECM
ECCM
CONFIRM
WARNING
ACTIVE ECM
PASSIVE ECM
DENIAL JAMMING
DECEPTIVE JAMMING
DENIAL JAMMING
DECEPTIVE JAMMING
COMINT
ELINT
ANTI-ESM (SIGSEC)
ANTI-ECM
COMSEC
ELSEC

نلاحظ في أسس الحرب الإلكترونية أن كلمة (الإجراءات) تكررت كثيرا وهي تعني باللغة الإنجليزية (MEASURES)، وأحيانا يطلق عليها لفظ «التدابير» وتعني كلمة الإجراءات في الحرب الإلكترونية:

كيفية استخدام أساليب محددة ومعدات إلكترونية متخصصة استخداما إلكترونيا في عمليات الحرب الإلكترونية (أو في عمليات أسس الحرب الإلكترونية) لكي نستطيع تحقيق الإستفادة والتأثير والحماية الإلكترونية، وبالتالي تحقيق أهداف الحرب الإلكترونية عامة وتحقيق أهداف أسس الحرب الإلكترونية بشكل خاص.

إذن فالإجراءات تعني كيفية استخدام :

أ ـ الأساليب المختلفة (الإلكترونية): مثل اختيار أرضية معينة (PLATFORM) لوضع أجهزة الحرب الإلكترونية عليها سواء على طائرات أو سفن أو آليات عسكرية. كذلك تحديد أوقات استخدام تلك الأجهزة، واختيار الأساليب الدفاعية والأساليب الهجومية.
وأيضاً تحديد أماكن وجود الأجهزة جغرافيا . . . الخ.

ب ـ المعدات الإلكترونية المختلفة: مثل أجهزة الإستقبال الراديوية والرادارية للرصد والمراقبة، ومعدات الإستطلاع والكشف، وأجهزة التشويش والمخادعة «التضليل الإلكتروني»، النصلات، أجهزة التشفير، والطائرات بدون طيار والكاميرات. . . إلخ . .

Radar		[illegible]	UHF		[illegible]	S		[illegible]	X	[illegible]	K	[illegible]	MILLIMETER	
ECM		[illegible]	B	C	[illegible]	E	F	[illegible] H	I	[illegible]		[illegible]	L	M
Wavelength (cm)	30	[illegible]	0 75 60 50 40		[illegible]	10 7		[illegible] 75 3		[illegible]	15	[illegible]	5 06 05 04 03	
Wavelength λ (dB/Meter)	4.	[illegible]	-30		[illegible]	-100		[illegible]		[illegible]		[illegible]	-230 -252	
Frequency (GHz)	0.	[illegible]	04 05 06 075		[illegible]	3		[illegible]	0 10	[illegible]	20	[illegible]	0 50 60 70 100	

شكل رقم (١/١٥)
يبين الشكل الطيف أو المجال الكهرومغناطيسي للترددات .

٣ ـ نبذة تاريخية عن الحرب الإلكترونية

كانت أساليب الحرب الإلكترونية تستعمل منذ بداية هذا القرن وبالأخص عندما استخدمت أجهزة الإتصالات اللاسلكية في الحروب، ولكن منذ الحرب العالمية الثانية أصبح موضوع الحرب الإلكترونية محل الإهتمام من حيث المعدات والأساليب.

تفيد المصادر[١] أن أول عملية في مجال الحرب الإلكترونية كانت في عام ١٩٠٥ خلال الحرب الروسية اليابانية في معركة (TSUSHIMA) عندما كانت سفن الإستطلاع اليابانية تراقب الأسطول الروسي عن كثب وترسل جميع المعلومات بالراديو إلى القيادة الرئيسية اليابانية وفي هذه الأثناء التقط أحد قادة الزوارق الروسية هذا الإرسال، فطلب الإذن باستعمال جهاز الإرسال الموجود بزورقه لإعاقة تلك الإرساليات ولكن طلبه قوبل بالرفض من قبل القيادة الروسية فاستمر إرسال المعلومات اليابانية وبعد فترة وجيزة استطاع أحد قادة الزوارق الروسية بدون إذن من قيادته التشويش على هذه الإرساليات ولكن بعد فوات الأوان إذ كانت المعركة قد وقعت وخسرها الروس .

أما في الحرب العالمية الأولى فقد استعملت أجهزة الإتصال وأجهزة نقل معلومات الإستطلاع بكثرة، إذ استطاعت إحدى السفن الإنجليزية عام ١٩١٤ أن ترسل بالراديو معلومات عن تحرك بعض القطع الحربية الألمانية في البحر الأبيض المتوسط ولكن بعد أن رصد الألمان تلك الإرساليات تمكنوا من التشويش الكامل عليها.

وفي عام ١٩١٦ وضع الإنجليز بعض موجدات إتجاه الإرسال قرب الأسطول الألماني، وخلال معركة جوتلاند حددت تلك الأجهزة موقع الأسطول وأبلغت القيادة الإنجليزية بذلك.

كانت البداية الحقيقية في الحرب العالمية الثانية لإستخدام أجهزة الحرب الإلكترونية المتخصصة ففي عام ١٩٣٩ استخدم الألمان طريقة «تقاطع موجات الإرسال فوق الهدف» (BEAM-INTERSECTION) لكي يقصفوا المدن الإنجليزية وخاصة أثناء

---

(١) مجلة INTERNATIONAL DEFENCE REVIEW بعددها الخاص عن الحرب الإلكترونية :SPECIAL SERIES ELECTRONIC WARFARE في عام ١٩٧٨م. صفحة ٧.

الليل، فوضع الإنجليز جهاز الإرسال (BROMIDE) ليقوم بتشويش مخادع ويجعل هذا التقاطع فوق مكان غير حيوي واختاروا لذلك بحر المانش، وفعلا وقع قصف الطائرات الألمانية على بحر المانش ولم تتضرر المدن الإنجليزية التي أراد الألمان قصفها.

واستخدم الحلفاء أجهزة التشويش والنصلات (CHAFF) للتشويش على الرادارات الألمانية عند الساحل الغربي الفرنسي، كما استخدمت في الحرب العالمية الثانية المناطيد والبالونات للتنصت والمراقبة والتصوير في عمق أراضي العدو.

في حرب كوريا : قام الأمريكيون بعمل بعض التعديلات على بعض الطائرات مثل (TB-25J) لكي تصبح طائرات تشويش على مواقع الدفاع الجوي الشيوعية، كما بدأ آنذاك وضع (TAIL WARNING RADAR) وهو جهاز يوضع في مؤخرة الطائرة لينذر عن وجود رادار معاد يتتبع الطائرة.

في حرب فيتنام : عندما استخدم الفيتناميون صواريخ سام ـ ٢ ضد طائرات الفانتوم الأمريكية أدخلت أمريكا تعديلات على طائرة (EB-66) القاذفة لتكون طائرة حرب إلكترونية (EW A/C) محملة بأجهزة تشويش ضد رادارات صواريخ سام ـ ٢، وبعدما نجحت هذه التجربة جرى تعديل وتركيب أجهزة التشويش على طائرات[1] (-F . 100, F-101, F-105 F-4).

وفي حرب ٦٧ استطاع الإسرائيليون التشويش الشامل على جميع أجهزة الإتصالات المصرية بسيناء قبل غزوها .

وفي عام ١٩٧١م استخدمت أمريكا أجهزة تشويش والنصلات (CHAFF) والصواريخ المضادة للرادارات الأرضية عندما أرادت قصف المدينتين الرئيسيتين لفيتنام الشمالية هانوي وهايبنوغ بالقاذفات (B-52) وقد كان ذلك التشويش مسلطا ضد صواريخ سام ـ ٢ والرادارات المستخدمة للمدافع المضادة للطائرات.

في حرب ١٩٧٣ م فوجيء الإسرائيليون باستخدام العرب لصواريخ سام ـ ٣، سام ـ ٦ ، والمدافع الروسية المضادة للطائرات (شيلكا ZSU-23-4 SHILKA) بكفاءة عالية، وكان لدى العرب أجهزة تشويش ، وأجهزة موجدة الإتجاه وفي الأيام الثلاثة الأولى خسرت إسرائيل حوالي ١٥٠ طائرة[2]. وقد استخدمت الطائرات الإسرائيلية طريقة الغطس

---

(١) مجلة INTERNATIONAL DEFENCE REVIEW عدد خاص عن الحرب الإلكترونية عام ١٩٧٨.
(٢) مجلة الوطن العربي الصادرة بباريس بتاريخ ١/١٠/١٩٨٢ م .

(DIVING) نحو صواريخ سام ـ ٦ للتخلص منها ، ولكنها لم تنجح .

وبعد هذه الخسائر الفادحة زودت أمريكا إسرائيل بأجهزة تشويش على رادارات تلك الصواريخ، فنجحت ـ بالتشويش في تخفيض الخسائر الإسرائيلية.

كما استخدمت إسرائيل النصلات (CHAFF) بنجاح في المعارك البحرية في حرب ١٩٧٣.

في حرب لبنان :

استخدم الإسرائيليون أجهزة وأساليب الحرب الإلكترونية بشكل كبير أدى إلى نجاح معظم عملياتهم الحربية (انظر الباب الرابع من هذا الكتاب).

وفي الثمانينات زاد الطلب على شراء أجهزة الحرب الإلكترونية من مراقبة وتشويش ومضادات التشويش خاصة بعد حرب فوكلاند وحرب لبنان، حتى أنه بلغت مصاريف دول العالم لشراء أجهزة الحرب الإلكترونية من الدول المتقدمة مليارات الدولارات سنويا وكان نصيب الأسد من هذه المليارات للشركات الأمريكية (أنظر الجدول المرفق)، كما أن إسرائيل كذلك ـ بعد الإستفادة الفنية من حروبها السابقة مع العرب والمنظمات الفلسطينية ـ بدأت بصناعة جميع أنواع أجهزة الحرب الإلكترونية من مراقبة وتشويش ومضادات التشويش وأخذت في بيعها لمختلف دول العالم وخاصة الطائرات بدون طيار (DRONES) و (R.P.V.) لدول أمريكا الجنوبية وقد بلغ عدد الدول التي تشتري أسلحة من إسرائيل أربعين دولة وكان مجمل صادرات إسرائيل من السلاح عام ١٩٨٣ هو ٦٥٠ ميلون دولار[١] .

وفي السنوات الأخيرة رأينا أن هناك طائرات خاصة تصنع فقط لأجهزة الحرب الإلكترونية مثل الأواكس الأمريكية والأواكس الروسية والنمرود الإنجليزية وطائرة عين الصقر الأمريكية، لتؤدي مهام مراقبة الإتصالات ومراقبة أجهزة الرادار الأرضية وأجهزة الملاحة والتشويش عليها، وكذلك مراقبة الغواصات والطائرات وتوجيه المقاتلات الصديقة نحوهم، مع العلم أن الفكرة الأساسية لهذا النوع من الطائرات هي رادارات للإنذار المبكر الجوي.

ويدخل المكوك الفضائي الأمريكي (SPACE SHUTTLE) ضمن معدات الحرب الإلكترونية. والفكرة الأساسية لعمل هذا المكوك أن يكون قريبا من الأقمار الصناعية

---

(١) مجلة المجلة الصادرة في لندن بتاريخ ١٩٨٤/٥/١٧ صفحة ٣١.

الروسية للتجسس عليها والتشويش إذا قضت الضرورة، وسيكون لدى أمريكا في أكتوبر ١٩٨٧م حوالي ٦٩ مكوكا فضائيا جاهزا للإستعمال وسوف يخصص ٢٤ مكوك منها للإستعمال العسكري[١].

ولاشك أن الأقمار الصناعية من أكثر الأجهزة إستعمالا من قبل الدول المتقدمة لعمليات الحرب الإلكترونية، والعسكرية حتى أن لدى روسيا حوالي ٥٥ قمرا صناعيا تستعمل منذ ١٩٨٠م في الأغراض العسكرية[٢].

ولما كان القمر الصناعي غير مرغوب في تحليقه فوق أرض العدو فقد استطاع السوفيت التشويش بنجاح عام ١٩٧٥م على قمر صناعي أمريكي للتجسس عندما سلطوا عليه أشعة ليزر ذات الطاقة العالية[٣].

وأخيرا سوف نتكلم عن حرب الفضاء أو كما يسمونها بـ (حرب النجوم) وهي باختصار استخدام مختلف المركبات والمكوكات الفضائية والأقمار الصناعية ـ إستخداماً هجومياً أو دفاعياً ـ في عمليات الحرب الإلكترونية والإستطلاعات والإنذار المبكر لتوجيه مختلف الأسلحة (وخاصة أسلحة الليزر) ولإقامة مراكز قيادة وسيطرة واتصال (C^3) فضائية لجميع القوات البحرية والجوية والبرية.

وسنذكر هنا بعض الفقرات التي وردت في تقرير من مجلة يو. أس. نيوز (U.S.NEWS) نقلته جريدة القبس الكويتية[٤]:

يقول التقرير :

من المهام الرئيسية لقيادة الفضاء في الوقت الحاضر، تنفيذ مجموعة من الوسائل الدفاعية لحماية المرافق الفضائية الأمريكية المعرضة للخطر، وتتضمن هذه الخطوات تقوية الأقمار الصناعية ضد الشحنات الإشعاعية الناشئة عن الرؤوس النووية، وجعلها أقل قابلية للتأثر بالتشويش الإلكتروني، وأكثر قدرة على القيام بمناورات في مدارات مختلفة لتحاشي مهاجمتها، وإطلاق مركبة فضاء يطلق عليها اسم « الطائر البارد » قادرة على البقاء صامتة ودون أن تكتشف، وذلك بجعلها تدور في مدارات عالية جدا لتكون بمثابة

---

(١) مجلة FLIGHT INTERNATIONAL ص٥٧ عدد ١٠/٧/١٩٨٢م.

(٢) المصدر السابق ص ٥٧.

(٣) كتاب INTELLIGENCE WARFARE.

(٤) العدد ٤٥٤٠ بتاريخ ٣/١/١٩٨٥م.

بدائل للأقمار الصناعية التي يمكن أن تدمر أثناء حدوث صدام، حيث تنزل هذه المركبات إلى مدارات أقل إرتفاعا وتقوم بالمهام التي كانت تقوم بها الأقمار المدمرة.

ويقول «ادوارد الدريج» وكيل وزارة الدفاع الأمريكية لشئون سلاح الجو: «أصبحت أنظمتنا الفضائية أساسية في عمليات قواتنا، ولهذا ينبغي لنا أن نحميها».

والإعتماد المتزايد الحالي للقوات المسلحة للدولتين العظميين على الفضاء يعني أن الـ ٢٥٠ قمرا صناعيا تقريبا التابعين لهاتين الدولتين، والتي تدور حول الأرض، لابد وأنها ذات يوم ستخوض صداما.

ويقول جورج كيوورث، المستشار العلمي للبيت الأبيض «حتى في حالة نشوب حرب محدودة جدا، فإننا سنعتمد بدرجة بالغة الحساسية على الفضاء، وتجاه موجوداتنا الفضائية ستكون في رأس أولوياتنا».

وحتى الآن، فإن ٨٠٪ من الإتصالات العسكرية الأمريكية تمر عبر الأقمار الصناعية، وفي كثير من الحالات تكون هذه الأقمار الوسائل الوحيدة للإتصال بين المراجع العليا في واشنطن وبين القوات البرية في الميدان، وقباطنة السفن في البحر وقادة الطائرات في الجو.

ومركبات الإنذار المبكر الفضائية، التي يمكنها كشف بداية تحرك الصاروخ من الأرض، تستطيع الآن أن تنذر بالهجوم فور بدئه، وكانت فترة الإنذار قبل هذه المركبات تقتصر على ٣٠ دقيقة، وهي الفترة التي تقطعها الرؤوس النووية العابرة للقارات حتى تقبل إلى الولايات المتحدة من الإتحاد السوفياتي، إلا أنه بفضل هذه المركبات صارت فترة الإنذار أطول بمقدار ١٥ دقيقة أخرى. والهدف من تطوير إمكانيات الكشف هذه، هو منع نشوب حرب من خلال تأمين عدم قدرة أي الدولتين العظميين على توجيه ضربة أولى مفاجئة للأخرى، بحيث لا تترك لها مجالا لضربة إنتقامية.

ومنذ أوائل الستينات سعت كل من الدولتين العظميين إلى استغلال المركبات الفضائية في التجسس على الأخرى، وذلك بطرق معقدة كثيرة، وأقمار الإستطلاع من خلال التصوير الفوتوغرافي الحديث، تستطيع التقاط صور لأشياء على الأرض بحجم علبة الحذاء، وتستطيع أقمار الإستطلاع (التجسس)، التي إعتادت على مراقبة المواقع المهمة كالتجمعات العسكرية، وأحواض بناء السفن، أن تميز بين المواقع الفعلية وبين

المواقع المقامة للتضليل، كما أنها قادرة على اختراق السحب والظلام.

والأقمار الصناعية الإلكترونية، التي يطلق عليها وصف «ابن مقرض» تستطيع التنصت على المكالمات الهاتفية، والإتصالات العسكرية اللاسلكية، والإشارات المنبعثة من الصواريخ عند إجراء التجارب عليها، كتلك التي تصدر عن الصواريخ السوفيتية عند عودتها إلى الأرض في منطقة شبه جزيرة كامشاتكا، ولهذا فإن هذه الأقمار أدوات مهمة للتحقق من التقيد باتفاقات الحد من التسلح.

والمركبات الفضائية ذات الأجهزة المتطورة الخاصة بالملاحة، لا تستطيع توجيه السفن والطائرات فقط، وإنما تستطيع كذلك توجيه الصواريخ نحو أهدافها، والأقمار الصناعية الخاصة بمراقبة الأحوال المناخية لها دور حاسم بالنسبة للقادة الذين يخططون لهجوم.

كما أنها تزيد من دقة إصابة الرؤوس النووية للصواريخ لأهدافها بتزويدها بمعلومات دقيقة عن سرعة الرياح في مواقع هذه الأهداف.

وقبل نهاية هذا العقد ستطرأ تحسينات أخرى كانت أكبر بكثير على مزايا أسلحة الحرب. وعلى سبيل المثال، فإن شبكة أقمار صناعية أمريكية تتألف من ١٨ قمرا ستصبح جاهزة للعمل في عام ١٩٨٨، ستسمح للطائرات والسفن الحربية والجنود في الميدان بتحديد مواقعهم بدقة متناهية، بحيث لا يتعدى مجال الخطأ أقداما قليلة وذلك في أي مكان في العالم. وأصبحت مثل هذه الدقة متوفرة بفضل ساعات ذرية مركبة في الأقمار الصناعية لا يتعدى مجال الخطأ فيها ثانية واحدة كل ٣٦ ألف سنة، وهذا النظام الذي يطلق عليه اسم (NAV. STAR GLOBAL POSITIONING SYSTEM) (أي نظام نافستار لتحديد المواقع على الأرض)، سيوفر دقة لا سابقة لها بالنسبة للأسلحة حين يجري استعمالها من جانب رجال المدفعية عند التصويب على الأهداف أو من جانب قادة قاذفات القنابل حين يشنون هجومهم في طقس سيء، أو في الليل، أو عند إطلاق الصواريخ من الغواصات، حيث يجري اعطاؤها آخر المعلومات عن مواقعها وهي في طريقها إلى أهدافها.

وهناك قمر صناعي للإتصالات يعمل بالإستعانة بأشعة الليزر صممته «وكالة مشاريع الأبحاث المتقدمة التابعة لوزارة الدفاع الأمريكية سيمكن الغواصات في المستقبل القريب من إجراء الإتصالات، بينما هي في أعماق المحيط، وحاليا لا تستطيع الغواصات إجراء أية إتصالات وهي تحت المياه العميقة، وينبغي أن تصعد إلى نقطة قريبة من سطح الماء لتسلم الرسائل، وذلك سيحد من سيطرة قادة الأسطول على تحركاتها، كما أن الغواصات من السهل على العدو كشفها حين تكون قريبة من سطح الماء الأمر الذي سيجعلها أكثر عرضة للخطر.

والسوفيت بدورهم، يحاولون إستغلال الفضاء بطريقة جديدة وفريدة فمحطتهم الفضائية المسامة «سارلوت ٧» التي يظل على متنها طاقم يتألف من ثلاثة أشخاص طول السنة تقريبا، تقوم بعدد من المهمات العسكرية، ومن بين هذه المهما كشف التغيرات القوية على سطح المحيطات من خلال استعمال أشعة الليزر وهو أمر يمكنهم من كشف الغواصات.

وبحلول عام ١٩٩٠ هناك انجاز أكبر محتمل، وهو وضع محطة فضاء سوفيتية تزن حوالي ١٠٠طن، ويعيش فيها حوالي ١٢ رائدا كونيا، بحيث تبقى في الفضاء بشكل دائم. فبالإضافة للأمور العملية التي توفر مثل هذه المحطة الفضائية الضخمة فرقة الإنجازات باهرة فيها، فإنه من الممكن أن تستعمل كذلك لأغراض الإستطلاع العسكرية، وتحديد الأهداف كما يمكن استعمالها في إجراء أبحاث على الأسلحة الفضائية بهدف تطويرها هناك.

Rank	Company	1985 Sales ($ Millions)	1986 Sales $ Millions)
1	Eaton	816 *	436
2	E-Systems	613	446
3	Loral	530	430
4	Grumman	500	431
5	Sanders	400	479
6	Raytheon/Sedco	398	340
7	Litton	350	231
8	Northrop	328	335
9	Lockheed	310 *	264 *
10	GTE-Sylvania	290 *	293 *
11	Racal (UK)	280	180
12	Thomson-CSF(France)	270	250
13	Westinghouse	250	271
14	ITT	200	195
15	Singer/DMS/EMS/HRB	200	80
16	TRW	170 *	169 *
17	Watkins-Johnson Co	165	162
18	General Electric	140	125
19	IBM	140 *	141 *
20	Tracor	125	103
21	Electronica (Italy)	119	88
22	American Electronic LabsInc.	105	79
23	Motorola	100	65
24	McDonnell Douglas	93	81 *
25	Magnavox	89	86
26	AEG-Telefunken (W. Germany)	89 *	81
27	Hughes Aircraft	85	79 *
28	ArgoSystems	80	64
29	Datatape	80	70
30	General Instruments	76	65
31	Adams-Russel	67	34
32	Elta-IAI (Israel)	62 *	55
33	AAI	60	60
34	Boeing	60 *	55
35	Ford Aerospace	60	19
36	Texas Instruments	59	55
37	Rohde & Schwarz (W. Germany)	58 *	40
38	Selenia (Italy)	56 *	56 *
39	Martin Marietta	55	48 *
40	Elisra (Israel)	50	60
41	Hollandse Signaalapparaten BV (Netherlands)	46 *	42 *
42	Fairchild Weston	43	67
43	GEC-Marconi (UK)	41 *	37 *
44	Tech-SymCorp/Tecom/Trak	36	34
45	Philips Elektronikindustrier (Sweden)	36	35
46	Sperry	35	—
47	Avantek	33 *	—
48	TCI	25	—
49	Cincinnati Electronics	22	21
50	Scientific Communications	14	13

(*) الجدول يبين أكبر خمسين شركة عالمية تصنع معدات وأجهزة الحرب الإلكترونية ومبيعات هذه الشركات لعامي ١٩٨٥م / ١٩٨٦م بملايين الدولارات الأمريكية انظر كتاب INTERNATIONAL COUNTERMEASURES HANDBOOK صفحة ٣٨٣ عام ١٩٨٧م.

الباب الثاني

أسس الحرب الالكترونية

١ ـ الأساس الأول للحرب الإلكترونية

استخبارات الإشارة (SIGNAL INTELLIGENCE (SIGINT

وكما ذكرنا في الباب الأول سنعرض بعض التعاريف المختلفة لموضوع واحد حتى نعرف كنه الموضوع من وجهات نظر متعددة ونذكر تعريفنا الذي يعكس وجهة نظرنا نحن :

١ ـ التعـريف في كتـاب : (THE INTERNATIONAL COUNTER MEASURES HANDBOOK) ص٥٧٢

(A GENERAL TERM WHICH INCLUDES BOTH COMMUNICATIONS INTELLIGENCE AND ELECTRONIC INTELLIGENCE)

ومعنى التعريف كالآتي :

استخبارات الإشارة هي (مصطلح عام يحوي كلا من : استخبارات الإتصالات والإستخبارات الإلكترونية) .

٢ ـ تعريف شركة (WATKINS-JOHNSON) الأمريكية :

(THAT DIVISION OF EW INVOLVING THE INTERCEPTION, PROCESSING AND ANALYSIS OF FOREIGN RADIATIONS)

ومعنى التعريف كالآتي :

استخبارات الإشارة هي «ذلك القسم في الحرب الإلكترونية المتضمن : الإعتراض والمعالجة والتحليل للإشعاعات الغريبة»

٣ ـ وهناك تعريف آخر يقول : (SIGINT IS THE EXPLOITATION OF FOREIGN SIGNAL EMISSIONS FOR INTELLIGENCE PURPOSES.)

ومعنى التعريف كالآتي :

استخبارات الإشارة هي «إستغلال إنبعاثات الإشارة الغريبة للأغراض الإستخبارية».

إستخبارات (« SIGNAL INTELLIGENCE « SIGINT).

وهي (تشمل إجراءات إستخبارات الإتصالات وإجراءات الإستخبارات الإلكترونية). فاستخبارات الإشارة تحوي الإستفادة من موجات إتصالات العدو الكهرومغناطيسية الفعالة (استخبارات الإتصالات) والإستفادة من موجات العدو الكهرومغناطيسية الفعالة في غير مجال الإتصالات(1)، وتأتي الإستفادة من:

مراقبة هذه الموجات المنبعثة من أجهزته (كالراديو والرادار مثلا) ورصدها وتحليليها للحصول على معلومات عن معداته وقواته ونشاطاته ومواقعة وتشكيلاته مما يساهم في إنجاح عملياتنا الحربية ويساند أسس الحرب الإلكترونية الأخرى.

وإستخبارات الإشارة تقوم عادة أثناء السلم بجمع أكبر قدر من المعلومات عن الأعداء حتى أن هذه المعلومات قد تؤثر على الحالة السياسية والإقتصادية والعسكرية بين الدول المجاورة والبعيدة.

وأجهزة استخبارات الإشارة يمكن أن تحمل على الطائرات والسفن والآليات الأرضية، العسكرية والمدنية، وبعض البلدان المهتمة بهذا الموضوع تكون استخبارات الإشارة لديها تابعة لقوات الطيرات والقوات البحرية والقوات البرية، كل يعمل في مجاله ثم تصب جميع هذه المعلومات في المركز الرئيسي للحرب الإلكترونية.

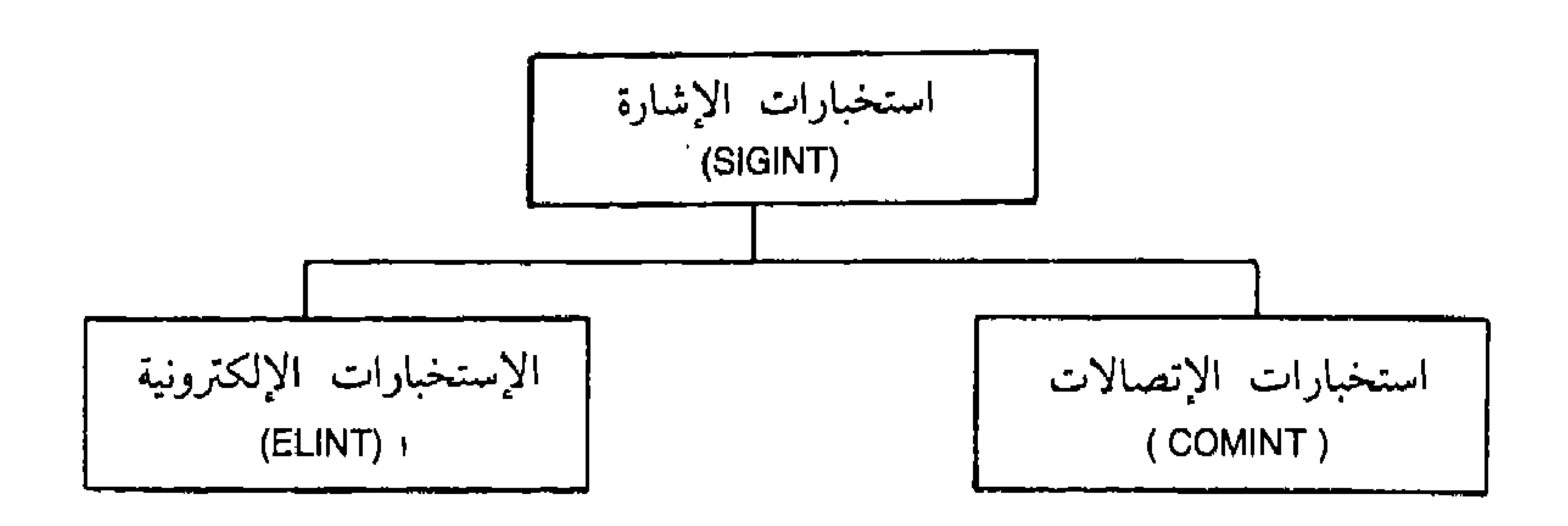
---

(1) ينقسم الإرسال الكهرومغناطيسي أو النظم الكهرومغناطيسية العسكرية MILITARY ELECTROMAGNA-TIC SYSTEMS إلى نوعين :

أ - اتصالات COMMUNICATIONS وهي فقط الموجات الكهرومغناطيسية المنبعثة من نظم الإتصالات والمنقولة عبر الأثير من راديو وتلكس وفاكسمل.. الخ (الاتصالات الهاتفية والتلغراف).

ب - غير اتصالات NON-COMMUNICATIONS وهي الموجات الكهرومغناطيسية المنبعثة من النظم غير الإتصالية والمنقولة عبر الأثير من (رادارات، أجهزة ملاحية، نظم تحكم بالأسلحة، .... الخ).

وتنقسم إستخبارات الإشارة إلى :



أ ـ إستخبارات الإتصالات : COMMUNICATIONS INTELLIGENCE (COMINT)

وقد وردت لها تعريفات عديدة، نقتطف بعضها فيما يلي :

١ ـ تعريف في كتاب : (WORLD ELECTRONIC WARFARE AIRCRAFT) (ص١٣).

ونصه : (DATA DEDUCED FROM THE STUDY OF HOSTILE SIGNALS TRAFFIC)

ومعنى التعريف كالآتي :

استخبارات الإتصالات هي «المعلومات المستنتجة من دراسة إشارات العدو».

٢ ـ تعريف في كتاب : (THE INTERNATIONAL COUNTER MEASURES HANDBOOK) ١٩٧٧/ ١٩٧٨ (ص٥٦٠)

نصه : (INTELLIGENCE DERIVED FROM THE INTERCEPTION OF ENEMY COMMUNICATIONS SIGNALS)

ومعنى تعريف إستخبارات الإتصالات هي : الإستخبارات المستمدة من إعتراض إشارات الإتصالات المعادية.

٣ ـ تعريف شركة (HUGHES) الأمريكية ونصه : (COLLECTION AND PROCESSING OF COMMUNICATIONS SIGNALS FOR INTELLIGENCE DATA) ومعنى تعريف

إستخبارات الإتصالات هي: تجميع ومعالجة إشارات الإتصالات بهدف إثراء المعلومات الإستخبارية.

٤ ـ تعريف آخر: (TECHNICAL AND INTELLIGENCE INFORMATION DERIVED FROM FOREIGN COMMUNICATIONS BY OTHER THAN THE INTENEDED RECIPIENTS)

ويعني هذا التعريف: المعلومات الفنية الإستخبارية المستمدة من الإتصالات الأجنبية من غير التلقي المقصود.

أما الآن سنورد تعريفنا نحن لإستخبارات الإتصالات (COMINT):

هي «العمليات التي تستخدم فيها أساليب ومعدات إلكترونية للإستفادة من موجات اتصالات العدو الكهرومغناطيسية الفعالة».

ويكون ذلك باستخدام أساليب إلكترونية محددةوأجهزة استقبال للرصدوالتنصت ومراقبة المعلومات المسموعة والمقروءة والمرئية المنبعثة من أجهزة إتصالات العدو اللاسلكية(١) على شكل موجات كهرومغناطيسية لتحليلها ومعرفة محتواها وتكون هذه المعلومات في مجال الإتصالات فقط كارساليات الراديو والتلكس وأجهزة اتصالات الميكروويف.. إلخ.

ويكون ذلك مثلا بوضع أجهزة استقبال الراديو الحساسة في أماكن تجمع العدو قرب الحدود للتنصت على إرسالياته وتحليلها لمعرفة مضمونها، كما يمكن وضعها على الطائرات والسفن لرصد تلك الإرساليات، أو داخل المدن لرصد إرساليات الجواسيس، أو وضع أجهزة التنصت الصغيرة (BUGGING DEVICES) في الغرف وافنائها أنظر شكل (٢/١)، أو وضعها على أجهزة كهربائية أو على الحيوانات الأليفة (مثل القطط والكلاب والعصافير.. الخ) التي يكثر وجودها بالقرب من العدو. وتعمل هذه الأجهزة ببطاريات تعمل باستمرار أو عند حدوث صوت (VOICE ACTIVATED) وذلك لحفظ البطاريات لمدة أطول.

---

(١) كذلك يمكن رصد ومراقبة المعلومات المنبعثة من أجهزة إتصالات العدو السلكية مثل التليفونات، وهي بالطبع موجات كهربائية وليست كهرومغناطيسية، لكن رصدها يعتبر ضمن عمليات استخبارات الإتصالات.



شكل رقم (٢/١)
يبين الشكل بعض الأماكن التي توضع بها أجهزة التنصت الدقيقة

ب ـ الإستخبارات الإلكترونية : ((ELECTRONIC INTELLIGENCE (ELINT))

لقد ذكرت المراجع تعريفات عدة للإستخبارات الإلكترونية، نذكر بعضها فيما يلي:

أ ـ تعريف في كتاب (WORLD ELECTRONIC WARFARE AIRCRAFT) نصه: (THE RESULT OF EVALUATING DATA DERIVED FROM ELECTRONIC RECONNAISSANDE).

ويعني التعريف أن الإستخبارات الإلكترونية هي:
نتيجة تحليل المعلومات المأخوذة من الإستطلاع الإلكتروني.

ب ـ تعريف شركة (HUGHES) الأمريكية:
نصه: (COLLECTION AND PROCESSING OF NON-COMMUNICATIONS ELECTRO-MAGNETIC SIGNALS FOR INTELLIGENCE DATA)

ويعني التعريف أن الإستخبارات الإلكترونية هي:
تجميع ومعالجة الإشارات الكهرومغناطيسية في غير مجال الإتصالات بهدف إثراء المعلومات الإستخبارية.

جـ ـ تعريف في كتاب: الحرب الإلكترونية» لكمال السعدي: يبين أن الإستخبارات الإلكترونية هي: جمع المعلومات الإلكترونية لمعرفة خصائص أنظمة سلاح الخصم وأجهزة الكشف التي يستخدمها».

ونخلص نحن إلى تعريف الإستخبارات الإلكترونية (ELINT) على النحو التالي:

هي **«العمليات التي تستخدم فيها أساليب ومعدات إلكترونية للإستفادة من موجات العدو الكهرومغناطيسية الفعالة في غير مجال الإتصالات»**.

ويكون ذلك بالرصد والتنصت ومراقبة المعلومات المرسلة من أجهزة العدو اللاسلكية لتحليلها ومعرفة محتواها، وهي جميع المعلومات التي لا تدخل في مجال الإتصالات: (NON-COMMUNICATIONS) ونعني بأجهزة العدو اللاسلكية: أجهزة الرادار والأجهزة الملاحية وأجهزة أشعة الليزر وأجهزة الأشعة تحت الحمراء الخ.

وعادة توضع أجهزة الإستخبارات الإلكترونية (ELINT EQUIPMENTS) على طائرات الإستطلاع وطائرات الحرب الإلكترونية (EW A/C) أو السفن أو الآليات الأرضية، أو المرتفعات التي توجد قرب الحدود لإلتقاط أكبر عدد ممكن من إرساليات العدو وموجاته الكهرومغناطيسية.

وعلى طول الحدود بين حلف الناتو وحلف وارسو بين ألمانيا الغربية وألمانيا الشرقية محطات ضخمة ليلتقط أحد الحلفين أية معلومات تنبعث من الحلف الآخر ثم يرسلها لتحليلها في الحال.

كما يعتبر التصوير من عمليات الحرب الإلكترونية وبالذات الإستخبارات الإلكترونية.

وكذلك المعدات الإستكشافية الحساسة مثل المنظار الحراري والمنظار المكبر وأجهزة كشف الإهتزازات وإفرازات الأجسام البشرية وأجهزة الكشف المغناطيسية.. الخ.

وكذلك وضع أجهزة تسمى (SONOBOUY) على سطح البحر للكشف عن الغواصات وتحدد أماكنها ومن ثم إرسال تلك المعلومات إلى القيادة، ويمكن قذف هذه الأجهزة من الطائرات أو السفن.

٢ ـ الأساس الثاني للحرب الإلكترونية

الإجراءات الإلكترونية المساندة

ELECTRONIC SUPPORT MEASURES (ESM)

وردت تعاريف عديدة للإجراءات الإلكترونية المساندة[1] (ESM) في الكثير من الكتب والمراجع المتخصصة، نذكر هنا بعضها :

١ ـ التعريف في الكتاب (INTELLIGENCE WARFARE) صفحة ٨١ :

(ACTIONS TAKEN TO SEARCH FOR, INTERCEPT, LOCATE, RECORD AND ANALYZE RADIATED ELECTROMAGENTIC ENERGY)

ومعناه : الإجراءات المتخذة للبحث والإعتراض وتحديد المكان وتسجيل وتحليل الطاقة الكهرومغناطيسية المنبعثة.

٢ ـ التعريف في كتاب «الحرب الإلكترونية» لكمال السعدي. صفحة ٩.

وهي عبارة عن إجراءات سلبية، تقوم بها تجهيزات معقدة وظيفتها استقبال الموجات الإلكترونية التي تبعثها أنظمة سلاح الخصم، وتحليلها، بهدف تمكين المراقب من معرفة ماهية مصدر الخطر وتقدير قيمته وبالتالي اتخاذ الإجراء الإلكتروني المضاد المناسب في الوقت المناسب: وتسمى إجراءات الإسناد الإلكتروني.

٣ ـ التعريف في كتاب (WORLD ELECTRONIC WARFARE AIRCRAFT)

« THE INTERCEPTION, LOCATION AND IDENTIFICATION, FOR IMMEDIATE TACTICAL USE, OF FOREIGN ELECTRO-MAGNATIC ENERGY »

ومعناه :

الإعتراض وتحديد المكان وتمييز الطاقة الكهرومغناطيسية الأجنبية للإستعمال التكتيكي السريع.

---

(١) في بعض الكتب تكتب: ELECTRONIC WARFARE SUPPORT MEASURES أو PASSIVE ELECTRONIC WARFARE (الحرب الإلكترونية السلبية).

٤ ـ تعريف شركة (RACAL COMMUNICATIONS) البريطانية:

(FOR INTERCEPTING AND LOCATING HOSTILE RADIO COMMUNTCATIONS AND WEAPONS SYSTEMS)

ويعني التعريف:

الإعتراض وتحديد مكان إتصالات الراديو ونظم الأسلحة المعادية.

أما الآن فسنورد تعريفنا نحن للإجراءات الإلكترونية المساندة (ESM) على النحو التالي:

هي «العمليات التي تستخدم فيها أساليب ومعدات إلكترونية للإستفادة من موجات العدو الكهرومغناطيسية الفعالة المنبعثة من معداته المختلفة».

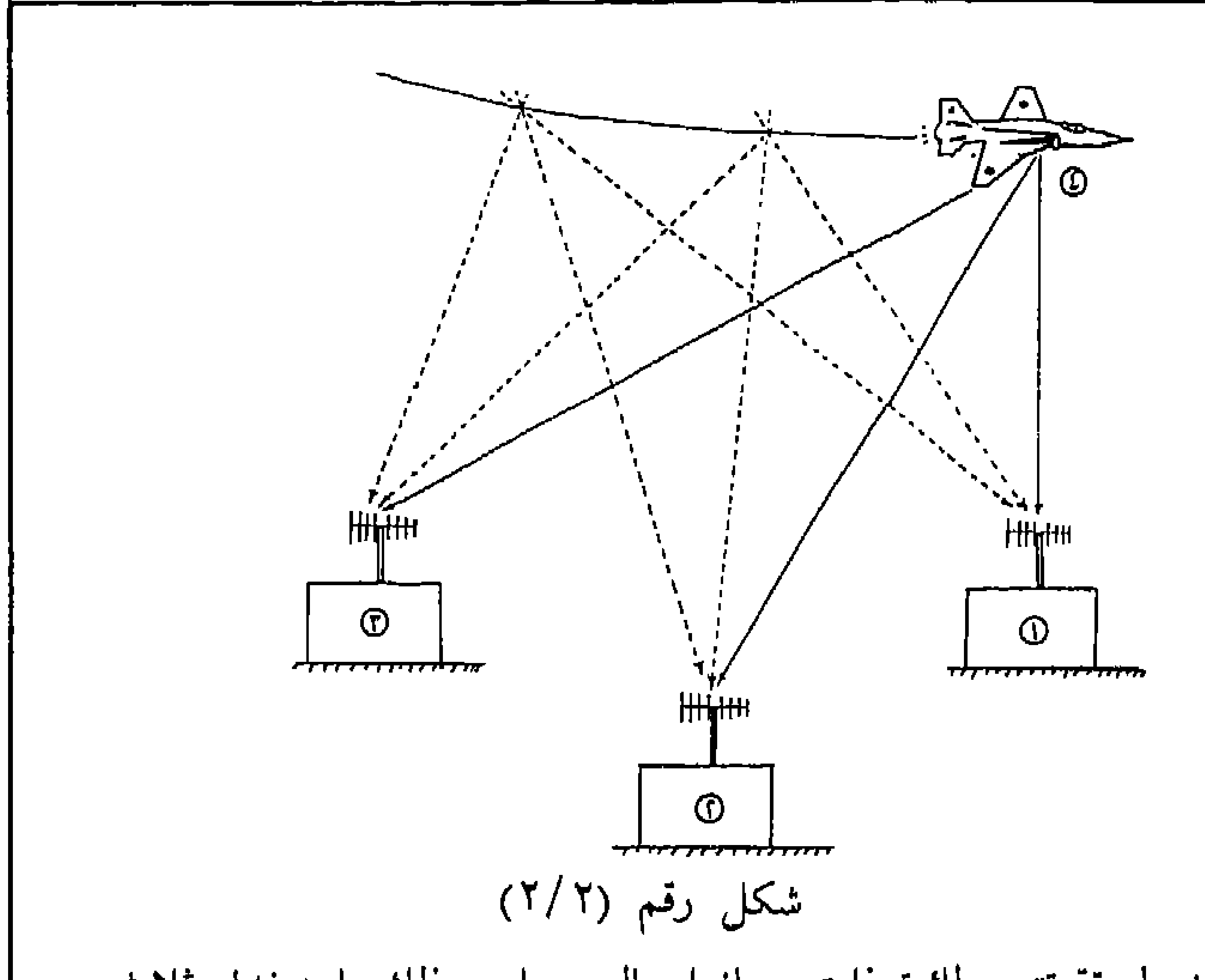
ويكون ذلك باستخدام أساليب إلكترونية معينة، وأجهزة استقبال إلكترونية (RECEIVERS) وهي أجهزة سلبية لرصد ومراقبة المعلومات المنبعثة من أجهزة العدو اللاسلكية المحمولة على الموجات الكهرومغناطيسية المنبعثة، لتحليلها ومعرفة قوة العدو ونشاطاته وتشكيلاته وتحركاته وخططه المستقبلية... الخ، ثم تحديد الموقف وإرسال المعلومات إلى الأساسين الثالث والرابع[1] (ECM, ECCM) لإتخاذ ما يمكن إتخاذه من إجراءات، وخاصة إجراءات التشويش، إذ دائما تكون الإجراءات الإلكترونية المضادة مستندة في عملها على الإجراءات الإلكترونية المساندة، كما أن معلومات الإجراءات الإلكترونية المساندة من شأنها أن تفيد خطط العمليات الحربية.

ومن أساليب ومعدات الإجراءات الإلكترونية المساندة إقامة محطات تنصت ومراقبة بها أجهزة إستقبال إلكترونية متطورة لرصد والتقاط جميع الذبذبات المنبعثة من أجهزة العدو ومعداته، ثم تحليلها ومعرفة معلوماتها. ومن المعدات المستخدمة أجهزة موجد الإتجاه (DIRECTION FINDER) (انظر شكل رقم ٢/٢)، لمعرفة موقع جهاز الإرسال ثم تحديد الأرضية المحمول عليها إذا كانت مثلا طائرة حربية أو هليوكبتر أو سفينة أو آلية برية... الخ.

ولمعرفة إتجاه إرسال العدو يكفي استعمال موجد إتجاه واحد، ولتحديد موقعه يجب استعمال موجدي إتجاه اثنين على الأقل وذلك بمراقبة سرعة تنقل جهاز الإرسال ونوعية

---

(١) سيرد ذكر هذين الأساسين بالتفصيل فيما بعد.



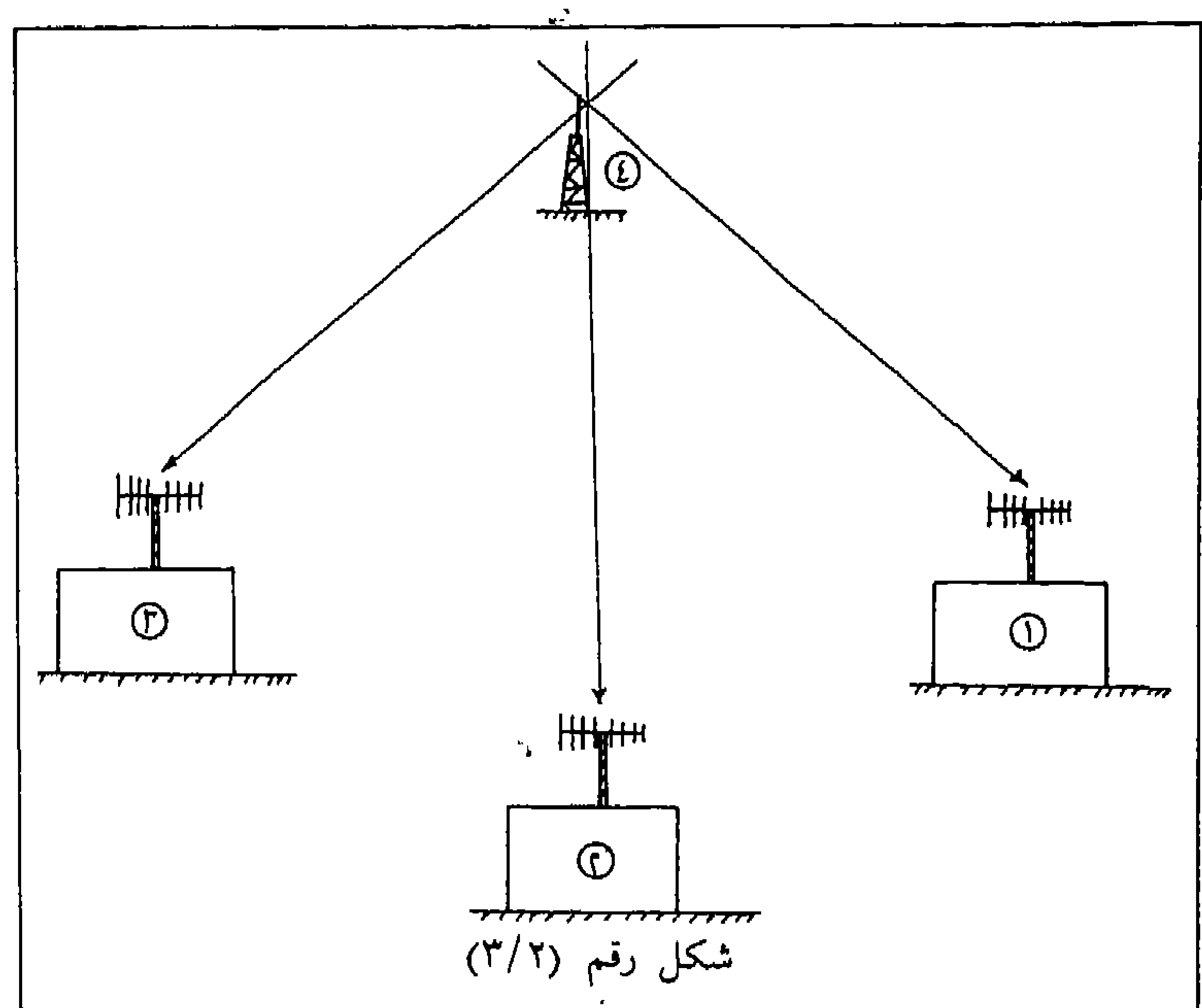
شكل رقم (٢/٢)

يبين طريقة تتبع طائرة ذات جهاز إرسال يرسل، وذلك باستخدام ثلاث أجهزة موجدة الإتجاه يعملون بطريقة (D.F. TRIANGULATION)

(١) و(٢) و(٣) أجهزة استقبال موجدة الإتجاه .
(٤) طائرة جهازها في حالة إرسال .

الذبذبات المستخدمة، فبتكرار هذه المراقبة والتحليل سوف نحصل على معلومات غاية في الأهمية (انظر شكل ٣/٢).

ولنضرب مثالاً على ذلك: من المعروف أن الدبابات والآليات البرية تستخدم دائما موجات معينة يطلق عليها الترددات التعبوية (TACTICAL FREQUENCIES) أي ذبذبات تعبوية وهي من ٢٠ ميغا هرتز إلى ٨٠ ميغا هرتز فبوضع أجهزة تنصت ومراقبة وموجدي إتجاه قرب حدود العدو لمراقبة تلك الذبذبات نستطيع أن نحدد مواقعه وتحركاته ، فإذا أراد الهجوم مثلاً سوف نلاحظ أن اتصالاته بتلك الذبذبات قد كثرت فجأة ، وأن مواقعه وتحركاته تقترب نحو حدودنا . وبتحليل المعلومات المنبعثة من أجهزته المرسلة يمكننا تحديد ما إذا كانت لديه نية للهجوم أو هي مجرد مناورة، وعادة يكون هناك «صمت إتصالات»



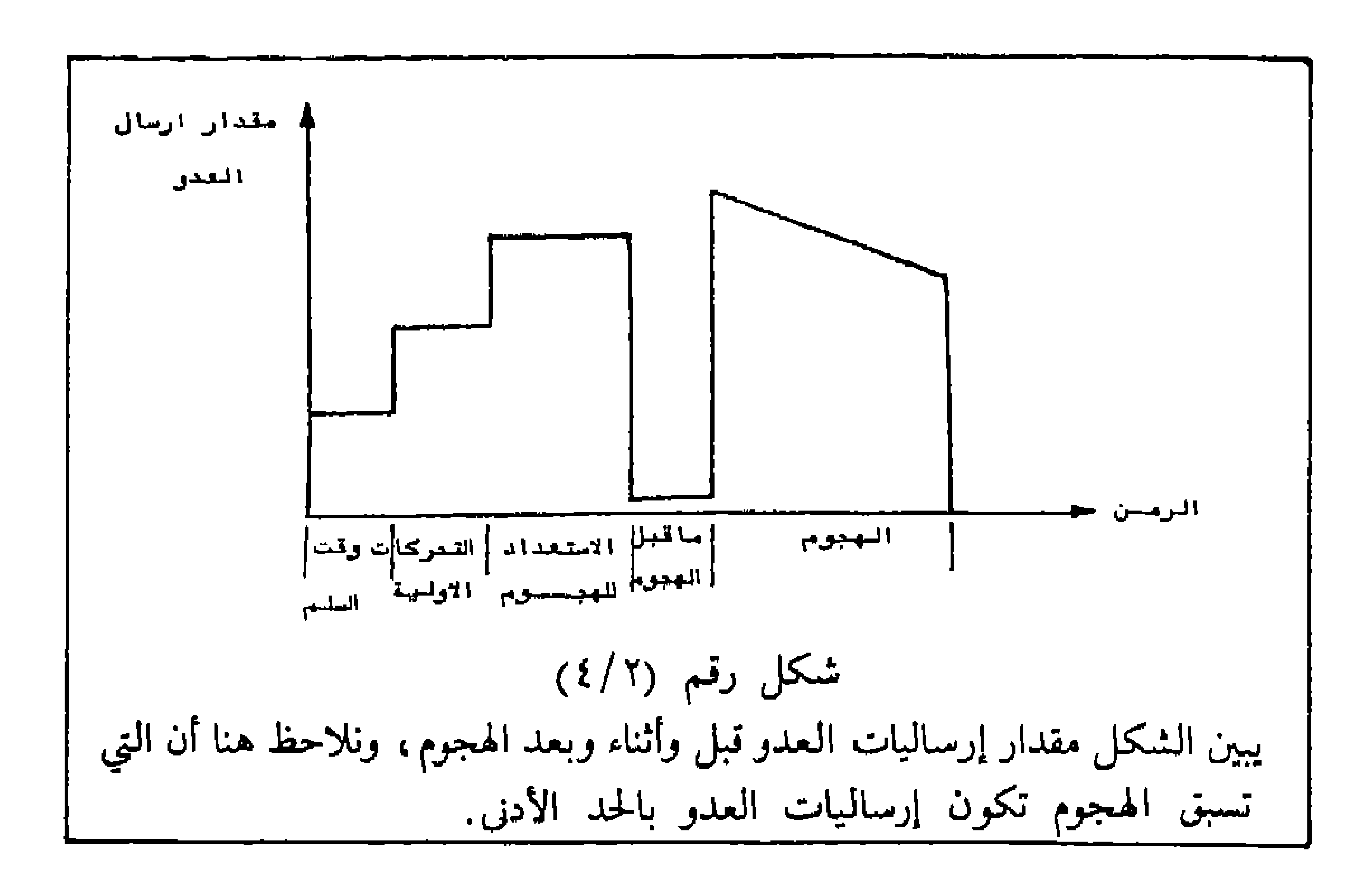
شكل رقم (٣/٢)

الشكل يوضح عملية تحديد مكان جهاز الإرسال باستخدام ثلاث أجهزة استقبال موجدة الإتجاه وذلك بطريقة (D.F. TRIANGULATION)

(١) و(٢) و(٣) أجهزة استقبال موجدة الإتجاه (تستقبل نفس ذبذبة جهاز الإرسال المراد تحديد إتجاهه ومكانه) .

(٤) جهاز إرسال .

(RADIO SILENCE) أو (صمت لاسلكي) حيث تقل اتصالات العدو فجأة فتتدنى إلى حوالي(١٪ ـ ١٠٪) من اتصالاته العادية وهذا يدل على احتمال أكبر للهجوم (انظر شكل رقم ٤/٢). وهذا بالضبط ما ذكره خبراء دول أوروبا الغربية عندما أراد الروس غزو تشيكوسلوفاكيا عام ١٩٦٨، وذلك بتنصتهم على الذبذبات التعبوية الروسية قرب الحدود التشيكوسلوفاكية.



شكل رقم (٢/٤)

يبين الشكل مقدار إرساليات العدو قبل وأثناء وبعد الهجوم، ونلاحظ هنا أن التي تسبق الهجوم تكون إرساليات العدو بالحد الأدنى.

نرى من تعريف الإجراءات الإلكترونية المساندة أنه تقريبا مطابق لمفهوم الأساس الأول (استخبارات الإشارة) لكن هناك اختلافات أهمها :

١ ــ تكون عمليات (استخبارات الإشارة) مستمرة ورتيبة على مدار الساعة وتكون في حالة السلم والحرب بدون انقطاع، أما عمليات (الإجراءات الإلكترونية المساندة) فهي عادة تكون لأوقات ولمهمات معينة وخاصة تكون في حالات التوتر الشديد مع العدو أوحالات الحرب .

٢ ــ معدات وأساليب (الإجراءات الإلكترونية المساندة) تكون مهيأة لعمليات سريعة من مراقبة وتحليل وغالبا ما يكون ناتج تلك العمليات رد فعل سريع كالإنذار مثلاً (WARNING) .

٣ ــ تعتمد عمليات الأساس الثالث (الإجراءات الإلكترونية المضادة) والأساس الرابع (المضادات الإلكترونية للإجراءات المضادة) على معلومات ونتائج عمليات (الإجراءات الإلكترونية المساندة) أكثر من عمليات (إستخبارات الإشارة) وذلك لأنها أكثر دقة وحداثة.

٤ ــ تستخدم عادة معدات الإجراءات الإلكترونية المساندة لتوثيق (CONFIRM) المعلومات السابقة سواء كانت من مصدر إستخبارات الإشاراة أو أي مصادر أخرى ، مثل

إستخدام معدات التصوير الجوي للتأكد من وجود معدات وأسلحة للعدو .

٥ ـ إستخبارات الإشارة ذات معلومات إستراتيجية وتكون عادة تابعة للهيئة العامة للإستخبارات التابعة مباشرة لوزارة الدفاع ، أما الإجراءات الالكترونية المساندة ذات معلومات تعبوية تكون عادة تابعة للعمليات الحربية في القوات البحرية والجوية والبرية مباشرة .

كما يطلق في بعض المصادر على الاستطلاع الألكتروني ELECTRONIC RECONNAISSANCE بأنه يتكون من (SIGINT + ESM) .

في جيوش الدول المتقدمة نرى أن قسم إستخبارات الإشارة منفصل تماما عن قسم الإجراءات الإلكترونية المساندة، ويكون القسم الأخير هذا دائما ملازما لقسم الإجراءات الإلكترونية المضادة، ولكن لابد أن نذكر أن قسم استخبارات الإشارة دائم الإتصال مع قسم الإجراءات الإلكترونية المساندة لتزويده بجميع المعلومات التي يحصل عليها .

وهكذا فإن الإجراءات الإلكترونية المساندة تفيدنا في معرفة قوات العدو وإمكاناته وأسلحته ومعداته وتحركاته . . وهذا بلاشك أمر مهم وضروري خاصة إذا كانت هناك دولة تناصبنا العداء . وقد اهتمت الدول المتقدمة منذ زمن طويل بهذه الإجراءات . فمثلا الولايات المتحدة الأمريكية قد أنفقت في عام ١٩٦٩ وحده ما يقارب مليار دولار لتوفير وسائل الإجراءات الإلكترونية المساندة، فتوفر لديها ما يتراوح بين ٧٠٪ و ٨٠٪ من المعلومات الضرورية عن جيوش الدول الأخرى بما فيها الجيوش العربية[١] .

كذلك معلومات الإجراءات الإلكترونية المساندة ومعلومات إستخبارات الإشارة تفيد بشكل كبير في معرفة قدرات وإمكانات العدو ومعرفة تهديدات العدو ووضع تقدير الموقف الإلكتروني للمعركة (E.O.B) بصورة أدق مما يساعد في وضع خطط أدق لمضادة خطط العدو وعملياته الحربية، وكذلك تساعد تلك المعلومات في وضع التخطيط المناسب لتوفير حاجاته المستقبلية لقواتنا وأسلحتنا .

---

(١) كتاب الحرب الإلكترونية لكمال السعدي طبعة ١٩٧٩ صفحة ١٣٢ .

المعلومات المراد الحصول عليها بأجهزة SIGINT & ESM

١ ــ معلومات الإتصالات :

أ ــ قدرة إرسال جهاز إرسال العدو (POWER TXION).
ب ــ التردد.
جـ ــ عرض المجال (BANDWIDTH).
د ــ نوع التضمين (MODULATION) ...FM, AM, FSK, USB, LSB
هـ ــ نوعية المعلومات صوتية (VOICE) أو بيانات (DATA).
و ــ نوعية قطبية هوائي الإرسال.
ز ــ هل هوائي الإرسال لجميع الإتجاهات أو لإتجاه واحد .
ح ــ إتجاه أو مكان جهاز إرسال العدو.
ط ــ نوعية أرضية جهاز الإرسال (طائرة ـ سفينة ـ آلية متحركة ـ مبنى).

٢ ــ معلومات الرادار :

أ ــ قدرة إرسال جهاز إرسال العدو (POWER TXION).
ب ــ التردد.
جـ ــ عرض النبضة . ((PULSE WIDTH (P.W.)
د ــ (PULSE REPETITION FREQUENCY).
هـ ــ (PULSE REPETITION PERIOD).
و ــ (« ARP » (ANTENNA ROTATION PERIOD)
ز ــ عرض الشعاع (BEAMWIDTH).
ح ــ قطبية هوائي جهاز الإرسال والإستقبال .
ط ــ هل الإرسال (PULSE OR CW) وكيفية عمل الرادار بالبحث والتتبع .
. . . الخ .

وهناك أساليب كثيرة لقسم الإجراءات الإلكترونية المساندة سنذكر بعضا منها ليتسنى لنا فهم تلك الإجراءات :

ويمكن تفصيلها على النحو التالي :
أ ــ معدات مراقبة الذبذبات والموجات.
ب ــ معدات الإستطلاع.
جـ ــ الكتب والمجلات ووسائل الإعلام.
د ــ الدول الصديقة.

أ ــ معدات مراقبة الذبذبات والموجات (FREQUENCY MONITORING) :

وهي عمليات استخدام الأجهزة الإلكترونية للرصد والتنصت على العدو ومراقبة جميع المعلومات التي يبعثها بأجهزته السلكية واللاسلكية وتحليلها والإستفادة منها في عملياتنا، ومن أجهزة التنصت أجهزةرصد الرادار لمعرفة خواصه وموقعه، كذلك أجهزة الراديو والسفن والغواصات والطائرات والقوات البرية، للوقوف على عملياتهم وتحركاتهم وماهية المعلومات المتناقلة بينهم لمعرفة نواياهم.

* نظام أو عملية الإجراءات الإلكترونية المساندة في محطة مراقبة ذبذبات الراديو (ESM STATION FOR FREQUENCY MONITORING).

نظام أو عملية الإجراءات الإلكترونية المساندة تنجز إما يدوياً أو أوتوماتيكياً، إذ تدار المحطة إما يدوياً من قبل الأشخاص المدربين مستعملين أجهزتهم بطريقة يدوية عادية خطوة خطوة (MANUAL SYSTEM) أو تدار ككل بطريقة سريعة الإنجاز باستخدام أجهزة الكمبيوتر (MICROPROCESSOR OR COMPUTERIZED SYSTEM)

وتتلخص هذه العملية أو النظام في هذه الخطوات[١] المرتبة :

١ ــ البحث SEARCH :

وهو أول خطوة لهذه المحطة، الهدف منها البحث عن أي إرسال معاد لإلتقاطه ورصده والتركيز عليه للتأكد من أنه إرسال معاد فعلا والحصول على أكبر قدر من المعلومات من هذا الإرسال وهذه المهمة إما أن تحدث عشوائياً لأي عدد من الذبذبات أو تحدث لذبذبات معينة من معلومات سابقة.

(١) نفس الخطوات المذكورة نستطيع أن نعمل بها في إستخبارات الإتصالات COMINT والإستخبارات الإلكترونية ELINT.

٢ ـ الإعتراض INTERCEPT :

وهي الخطوة الثانية فبعد أن وجدنا الإرسال وتأكدنا أنه معاد، نقوم بتحديد خواص الإرسال من حيث :
الذبذبة، التضمين، طاقة الإرسال، وقت الإرسال.. الخ.

٣ ـ التحليل AYALYSIS :

وهو الخطوة الثالثة الهدف منها تحليل وتفنيد المعلومات المرسلة لمعرفة مضمونها كما نستطيع معرفة نوع الجهاز المرسل ووظيفته بالنسبة لقوات العدو (كأن يكون رادار موجه للصواريخ FIRE CONTROL RADAR).

٤ ـ تعيين الموقع LOCATION :

وهو الخطوة الرابعة لتحديد إتجاه وموقع جهاز إرسال العدو ولو بالتقريب ويكون هذا بإستعمال موجد الإتجاه (DIRECTION FINDER «DF») ، ولتحديد اتجاه جهاز إرسال العدو يستخدم موجد إتجاه، أما لتحديد موقع الجهاز فيستخدم موجد إتجاه إثنان على الأقل، وأيضا يمكننا تحديد نوعية الأرضية المحمول عليها أجهزة إرسال العدو سواء كانت طائرة أو سفينة أو آلية برية وذلك بملاحظة سرعة تنقل جهاز الإرسال.

٥ ـ التدوين RECORDING :

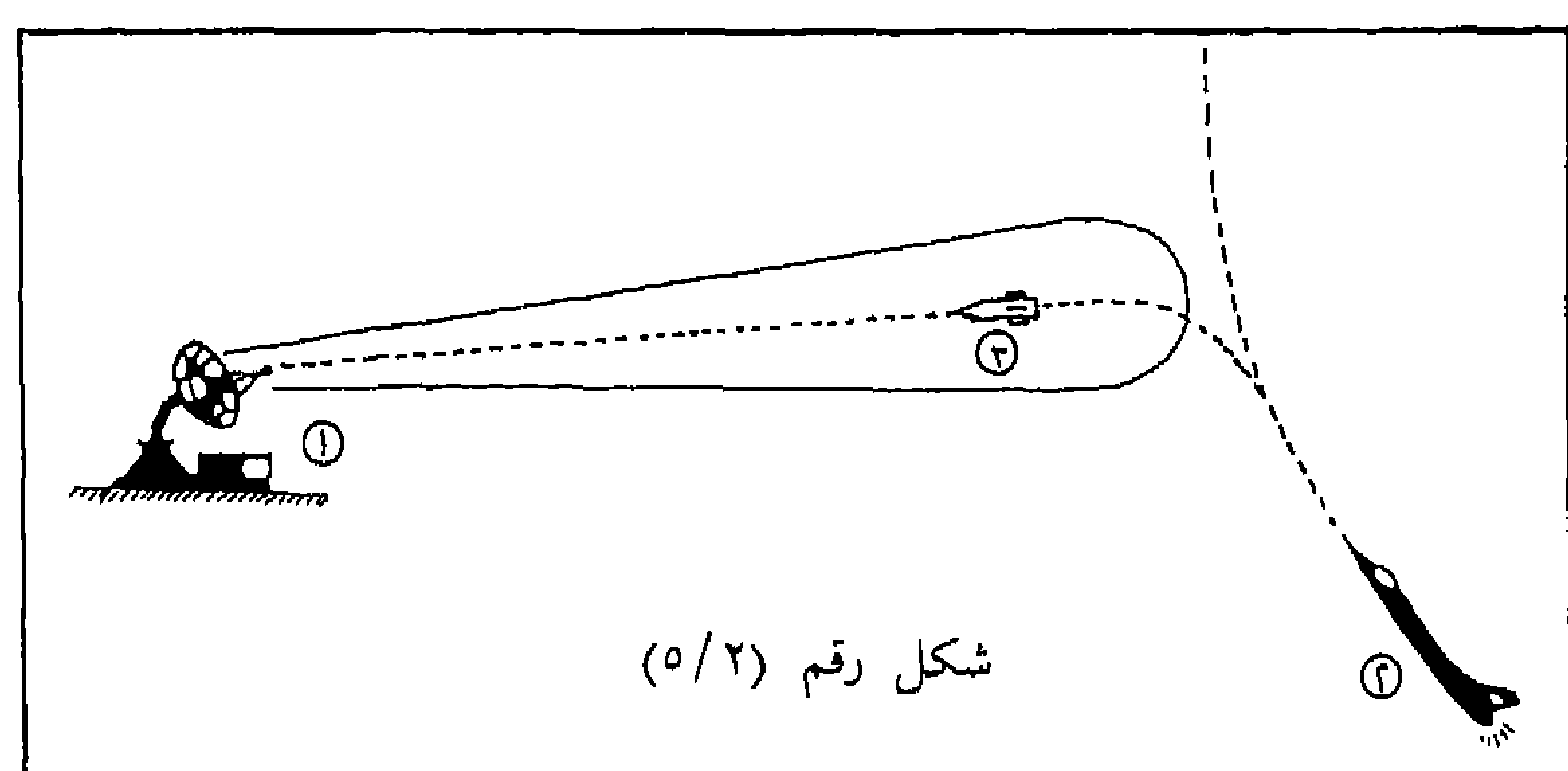
وهو الخطوة الخامسة الهدف منها تدوين جميع المعلومات التي قد حصلنا عليها من الخطوات السابقة، ويكون لهذا التدوين أنماط عديدة منها :
الأوراق والملفات، الصور الفوتوغرافية أو أشرطة الفيديو، أشرطة التسجيل، التخزين في ذاكرة جهاز الكمبيوتر.

وبعد ذلك تكون هذه المعلومات جاهزة للإستفادة منها في العمليات العسكرية، والإجراءات الإلكترونية المساندة المستقبلية، والإجراءات الإلكترونية المضادة، والمضادات الإلكترونية للإجراءات المضادة.

طبعاً أثناء العمل الفعلي في محطة مراقبة ذبذبات الراديو قد لا تتم الخطوات

بالترتيب الذي بيناه بالضبط، إذ قد تنقص خطوة، أو تسبق خطوة خطوة أخرى ولكن الهدف هو المحاولة لإنجاز جميع هذه الخطوات بشكل أو بآخر من أجل الحصول على أكبر قدر من المعلومات للإستفادة منها وكلما كانت تلك المعلومات دقيقة كانت الإستفادة أكبر .

وهناك أجهزة للإجراءات الإلكترونية المساندة سريعة الأداء للخطوات التي ذكرناها فتقوم بالبحث والإعتراض. . . إلخ وتقوم أوتوماتيكياً بإجراء إنذار كجهاز (REAR WARNING RADAR « RWR ») المركب على الطائرات) أو بإطلاق الصواريخ المضادة للإرسال: (ANTI-RADIATION MISSILE) انظر الشكل رقم (٢/٥). أو لتشغيل أجهزة التشويش أوتوماتيكياً (انظر التشويش المعاد).



شكل رقم (٢/٥)

يبين الشكل كيفية إطلاق صاروخ مضاد للإرسال إلى مصدر الإرسال (الرادار) وهو بالطبع صاروخ سلبي (PASSIVE MISSILE).

١ ـ رادار كشف ذو إرسال وإستقبال.
٢ ـ طائرة معادية تطلق الصاروخ.
٣ ـ صاروخ مضاد للإرسال (ANTI-RADIATION MISSILE (ARM))

ب ـ معدات الإستطلاع :

ويعرف الإستطلاع بعملية إستكشاف أراضي العدو لمعرفة أنواع وتحركات وأعداد قواته وأسلحته.

ويكون استخدام الطائرات المجهزة بأجهزة تصوير وأجهزة تصوير حساسة للأشعة تحت الحمراء (INFRARED SENSORS) وأجهزة رصـد رادارية.. الخ، لجلب المعلومات التي تفيد العمليات الحربية وتعطي صورا ملموسة عن تحركات العدو وتجمعاته، وأغلب الأجهزة والمعدات التي تستخدم في الاستطلاع الجوي هي أجهزة الموجات الكهروبصرية. (ELECTRO-OPTIC EQUIPMENT) كما يستخدم القمر الصناعي والمكوك الفضائي لنفس الغرض.

جـ ـ الكتب والمجلات والصحف ووسائل الإعلام الأخرى :

وهي الوسائل الإعلامية التي تحوي معلومات عن ماهية أجهزة العدو وإمكاناته وأسلحته وخططه ويقال أن حوالي ٨٠٪ من معلومات الدول يحصل عليها من وسائل الإعلام. لذا نرى كثيرا من المنظمات والوكالات العالمية والمخابرات تركز على هذه الوسائل فمثلا وكالة الإستخبارات المركزية الأمريكية CIA (CENTRAL INVESTIGATION AGENCY) تحصل يوميا على جميع كتب ومجلات وصحف العالم بأسره، وسنضرب مثالا بسيطا على ذلك:

في حرب لبنان بعد أن جلبت سوريا في عام ١٩٨٢، ١٩٨٣ بطاريات صواريخ سام ٨ وسام ٥ السوفيتية وكانت هذه الصواريخ متقدمة وجديدة ولم تكن هناك معلومات عنها إلا القليل جدا. حصلت الإستخبارات الإسرائيلية على خبر مفاده أن:

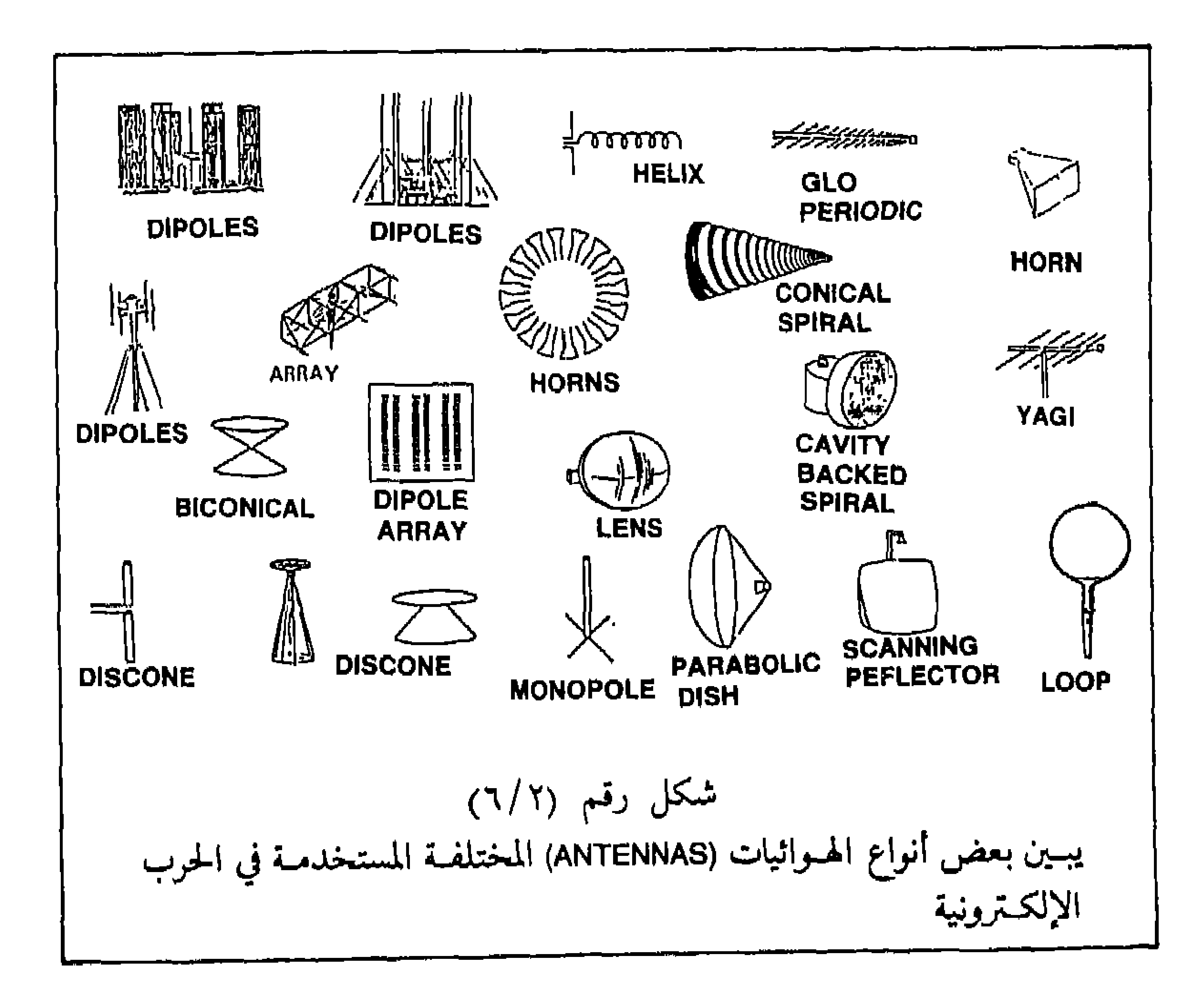
١ ـ أن صواريخ سام ٨ لا تستطيع الإنطلاق عند تنقلها من مكان لآخر، مع العلم بأنها (MOBILE BATTERY MISSILE)، فظلت إسرائيل تراقب تلك البطاريات عن كثب ولما رأتها في حالة انتقال كانت طائرات إسرائيلية جاهزة فقصفت الصواريخ وهي متحركة فحطمت بطاريتين من بطارياتها.

٢ ـ صواريخ سام ٥ جلبت إلى سوريا للتصدي للطائرات الإسرائيلية الإستكشافية وطائرات الإنذار المبكر مثل (E-2C HAWKEYE) البعيدة المدى وقد تبين للإسرائيليين أن لصواريخ سام ٥ نقطة ضعف تتمثل في أنها لا تتصدى للطائرات

ذات التحليق المنخفض، ومن ثم هاجمتها على طريق دمشق ـ بيروت بطائرات ذات تحليق منخفض، وحطمت إحدى بطارياتها.

د ـــ الدول الصديقة : إمكانية تبدال هذه النوعية من المعلومات بين الدول الصديقة.

وأخيراً يجب أن تتجمع كل المعلومات التي قد تم الحصول عليها من أقسام ومحطات (إستخبارات الإشارة) كمحطات مراقبة الذبذبات والإستطلاع الجوي والأشخاص المدربين ووسائل الإعلام .. إلخ، يجب أن تصب كل هذه المعلومات في مركز الإجراءات الإلكترونية المساندة الرئيسية وذلك حتى تصنف وتدقق ثم ترسل للقيادة للإستفادة من تلك المعلومات وكذلك للأساس الثالث (الإجراءات الإلكترونية المضادة) والأساس الرابع (المضادات الالكترونية للإجراءات المضادة) لرفع كفاءة عملياتها .



شكل رقم (٦/٢)
يبين بعض أنواع الهوائيات (ANTENNAS) المختلفة المستخدمة في الحرب الإلكترونية

٣ ـ الأساس الثالث

الإجراءات الإلكترونية المضادة

ELECTRONIC COUNTER MEASURESECM(1)

وردت تعاريف عديدة للإجراءات الإلكترونية المضادة (ECM) في الكثير من الكتب والمراجع المتخصصة، نذكر هنا بعضها :

١ ـ التعريف في كتاب (INTELLIGENCE WARFARE) صفحة ٨١

(ACTIONS TAKEN TO PREVENT OR REDUCE THE ENEMY'S EFFECTIVE USE OF THE ELECTROMAGNATIC SPECTRUM)

ويعني :

الإجراءات المتخذة لمنع أو تقليل استخدام المجال الكهرومغناطيسي الفعال المعادي .

٢ ـ التعريف في كتاب الحرب الإلكترونية لكمال السعدي صفحة ٩

« وهي مجموعة الإجراءات الإيجابية التي تتخذ في مواجهة أسلحة الخصم ».

٣ ـ التعريف في كتاب (WORLD ELECTRONIC WARFARE AIRCRAFT)

(ACTION AGAINST AN ELECTRO-MAGNETIC SOURCE, DESIGNED TO RENDER IT INEFFECTIVE).

ويعني هذا التعريف :

الإجراء المضاد لمصدر كهرومغناطيسي والمصمم ليجعل المصدر غير فعال .

٤ ـ تعريف شركة (RACAL COMMUNICATIONS LIMITED) البريطانية

(FOR DISRUPTING HOSTILE RADIO COMMUNICATIONS AND WEAPONS SYSTEMS).

ويعني هذا التعريف:

« لتمزيق إتصالات الراديو وأنظمة الأسلحة المعادية ».

---

(١) وقد يطلق على هذه التسمية في بعض الكتب: :ACTIVE ELECTRONIC WARFARE (الحرب الإلكترونية الإيجابية).

أما الآن فسنورد تعريفنا نحن عن الإجراءات الإلكترونية المضادة (ECM) على النحو التالي :

هي « **العمليات التي تستخدم فيها أساليب ومعدات إلكترونية للتأثير على معدات العدو الإلكترونية الفعالة لمنع أو تقليل إستفادته منها** » .

فالتأثير هنا يقصد به مختلف أنواع التشويش والمخادعة والتضليل والتداخل الإلكتروني الموجه نحو أجهزة وأنظمة ومعدات العدو المستقبلة (RECEIVERS) وذلك لتعميتها أو لمنع فعاليتها أو على الأقل التقليل من تلك الفعالية وبالتالي منع استفادة العدو منها جزئياً أو كلياً .

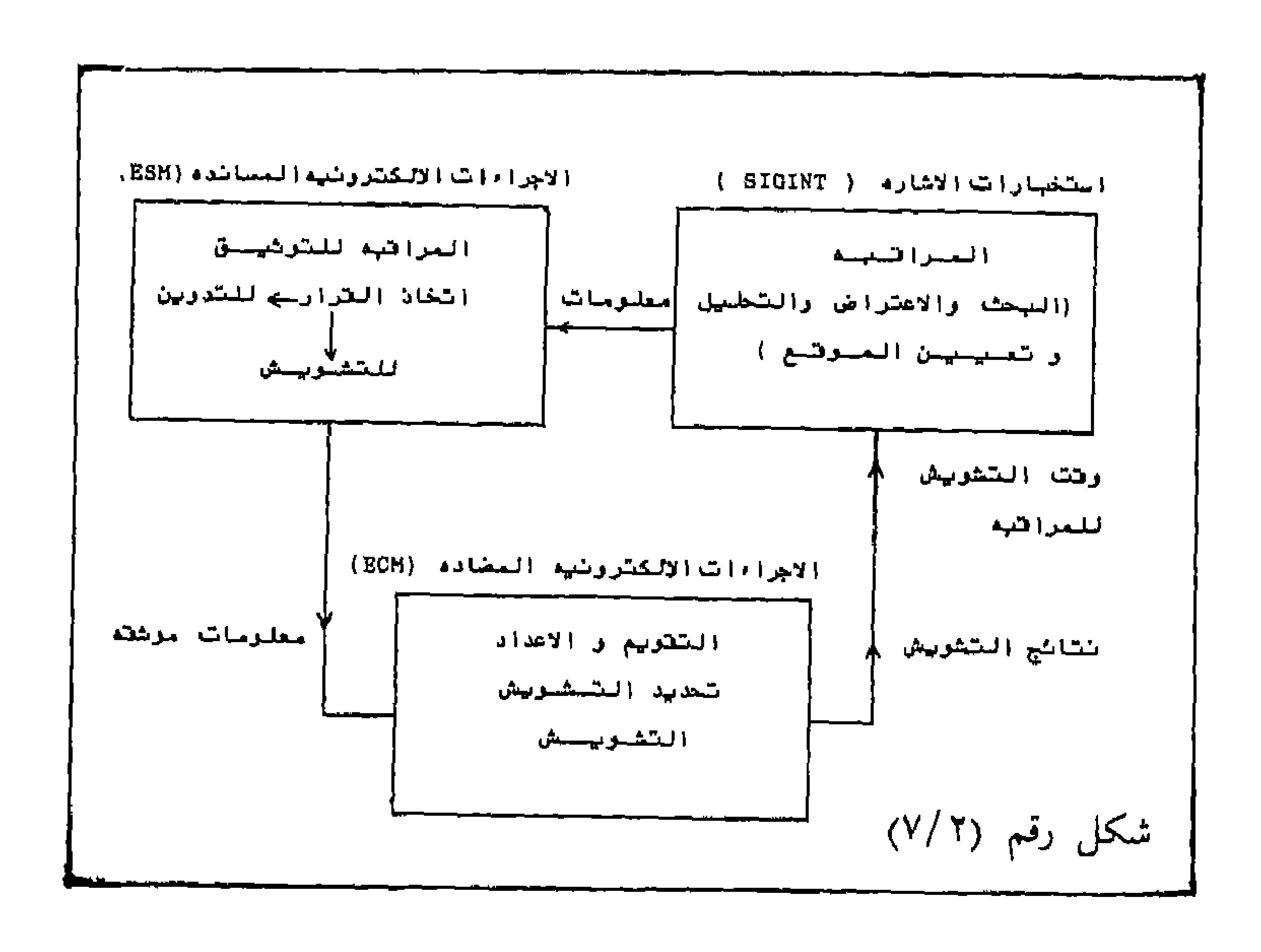
إذ بالتشويش والمخادعة الإلكترونية لأجهزة العدو من إتصالات ورادارات وأجهزة ملاحية . . الخ ، نجعله يتخذ إجراءات عملية خاطئة أو غير دقيقة يكون من شأنها التأثير على دقة عملياته الحربية .

ويكون لهذا التأثير فائدته الكبرى إذا نجحنا في تركيز التشويش والمخادعة الإلكترونية على القيادة والسيطرة والإتصالات (C^3) التابعة للعدو لإرباك عملياته الحربية .

وتُستعمل الإجراءات الإلكترونية المضادة عادة في حالة الحرب أو التوتر الشديد بين دولتين وخاصة عند الهجوم على العدو.

فإذا أريد مثلا قصف موقع ما للعدو بطائرة ويوجد في ذلك الموقع بطارية صواريخ موجهة مضادة للطائرات (SAM) فبإستخدام الإجراءات الإلكترونية المضادة (كجهاز التشويش على الرادارات) يمكن أن تشوش وتعمي رادار تلك البطارية ، وبالتالي يكون من السهل قصف تلك البطارية ، كما يمكن استخدام جهاز ذي تشويش مخادع ليظهر على شاشة الرادار لبطارية الصواريخ وكأنه أكثر من هدف أو كأن الهدف قريب جداً أو بعيد جداً فيتخذ العدو بذلك إجراء غير دقيق ، ويمكن كذلك التشويش على إتصالات قيادة جيش ما ، مما يؤثر على دقة عملياته ويطلق على الإجراءات الإلكترونية المضادة بشكل عام والإجراءات الإلكترونية المضادة الإيجابية بشكل خاص التشويش (JAMMING) ويجب أن نعلم أنه دون الحصول على معلومات من الأساس الأول (SIGINT) والأساس الثاني (ESM) فإننا لا نستطيع أن ننجح في استخدام الإجراءات

الإلكترونية المضادة للتأثير على أجهزة العدو بالصورة المطلوبة إذ أن الأساس الأول والثاني لا غنى عنهما لنجاح الأساس الثالث. وعمليا وبشكل عام إذا وضعنا الأساس الأول والثاني والثالث للحرب الإلكترونية على شكل خطوات كما هو مبين بالشكل رقم (٧/٢) سنلاحظ أن الأساس الأول استخبارات الإشارة (SIGINT) يزود الأساس الثاني « الإجراءات الإلكترونية المساندة » (ESM) مباشرة طوال الوقت من مراقبة وتحليل لإشارات العدو، فيقوم الأساس الثاني كذلك منفردا بالبحث والإعتراض لإشارات العدو وتحليلها والتأكد من معلومات الأساس الأول ومن ثم يقوم بتجميع كل هذه المعلومات لتقدير الموقف الإلكتروني للمعركة (E.O.B).



شكل رقم (٧/٢)

ثم ترسل المعلومات محددة الخواص (ذبذبة وتضمين.. الخ) إلى التدوين لتحفظ لعمليات إلكترونية في المستقبل، أو ترسل إلى الأساس الثالث (الإجراءات الإلكترونية المضادة) للتشويش أو المخادعة، فيستقبلها الأساس الثالث ويقوم بتقويم المعلومات والإعداد للتشويش ثم تحديد التشويش من حيث نوع جهاز التشويش

(ونوعية أرضية جهاز التشويش PLATFORM وقت التشويش، مدة التشويش. . الخ)، ثم يقوم بتنفيذ التشويش عمليا موجها إلى أجهزة ومعدات العدووأنظمة أسلحته المستقبلـة (RECEIVERS) يتخلل عملية التشويش فترات قصيرة جداً من المراقبة للتأكد من أن العدو لم يطفىء أو لم يغير خواص إشارته أو اتصالاته (من ذبذبة وتضمين. . الخ). فإذا أطفأ العدو معداته فيجب إطفاء ووقف التشويش، وإذا غير العدو بعض خواص إشارته أو اتصالاته يجب أن تتغير خواص التشويش لتلائم إشارة العدو حتى يكون التشويش مؤثرا وفعالا، وهكذا. . .

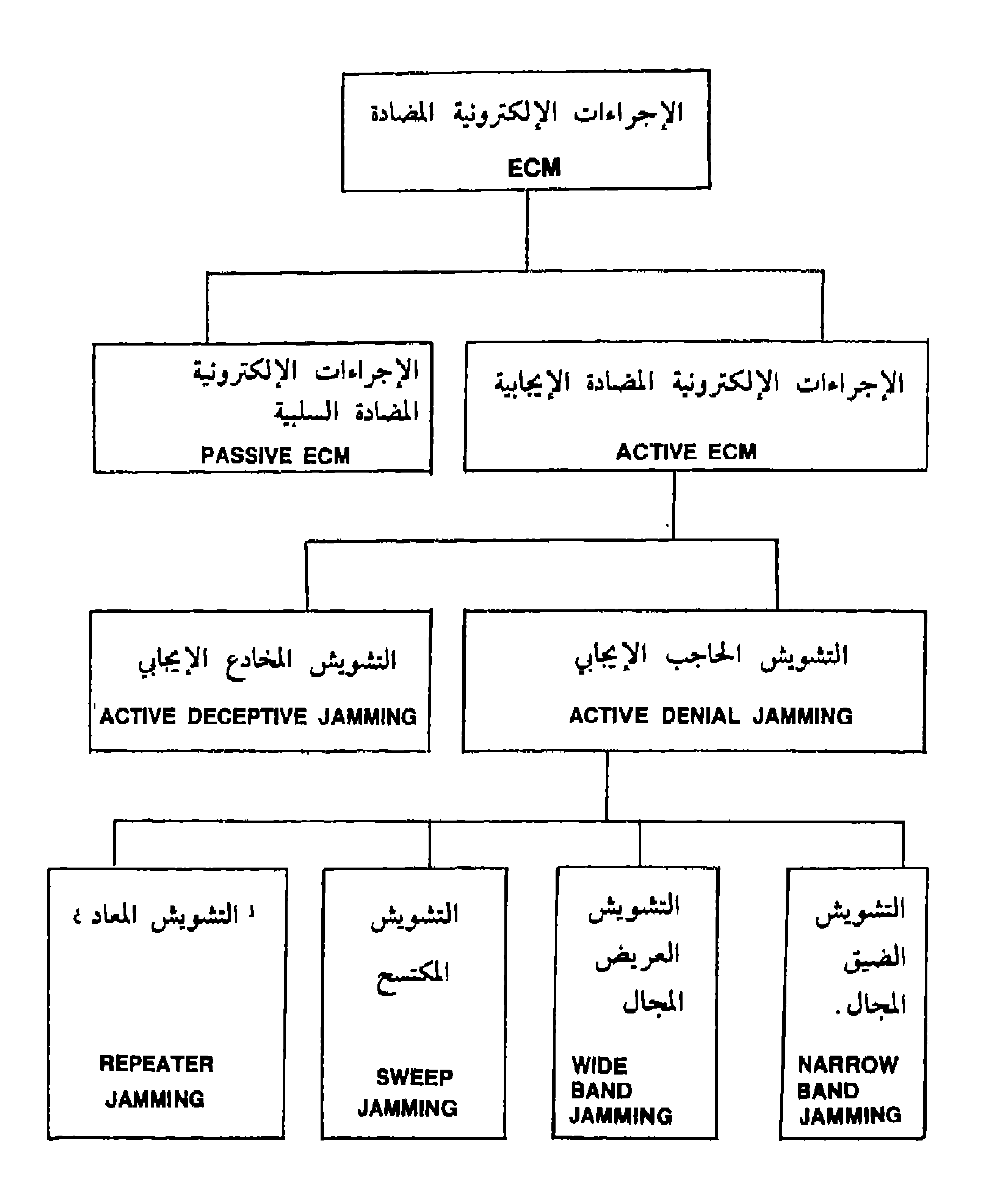
وهذه الفترات القصيرة جداً من المراقبة في الأساس الثالث تسمى (LOOK THROUGH) ومن هذا المثال البسيط نرى أن تلك الأسس تكمل بعضها البعض.

وعلى ذلك فإنه إذا ما استخدمت الإجراءات الإلكترونية المضادة استخداما مثاليا ضد أجهزة وقوات العدو فإننا نحقق ما يسمى بحالة القتل الناعم (SOFT KILL).

وبما أن العدو يكون عندئذ في حالة من العمى والإرتباك وهي حالة غاية في الخطورة بالنسبة له، فإن الفرصة تكون مواتية للقضاء عليه بأقل تكلفة وأقل ضرر من جانبنا وبأكثر تدمير ممكن له ولمعداته .

وهذه التسمية «القتل الناعم» تبين الاختلاف بين استخدام الإجراءات الإلكترونية المضادة واستخدام الأسلحة الإعتيادية (CONVENTIONAL WEAPONS) (من قنابل ومدافع وصواريخ. . الخ) مباشرة التدمير والتي تسمى (HARD KILL).

وتنقسم الإجراءات الإلكترونية المضادة (ECM) إلى :


الإجراءات الإلكترونية المضادة
ECM
الإجراءات الإلكترونية المضادة الإيجابية
ACTIVE ECM
الإجراءات الإلكترونية المضادة السلبية
PASSIVE ECM
التشويش الحاجب الإيجابي
ACTIVE DENIAL JAMMING
التشويش المخادع الإيجابي
ACTIVE DECEPTIVE JAMMING
التشويش الضيق المجال.
NARROW BAND JAMMING
التشويش العريض المجال
WIDE BAND JAMMING
التشويش المكتسح
SWEEP JAMMING
التشويش المعاد
REPEATER JAMMING

أ ــ الإجراءات الإلكترونية المضادة الإيجابية :

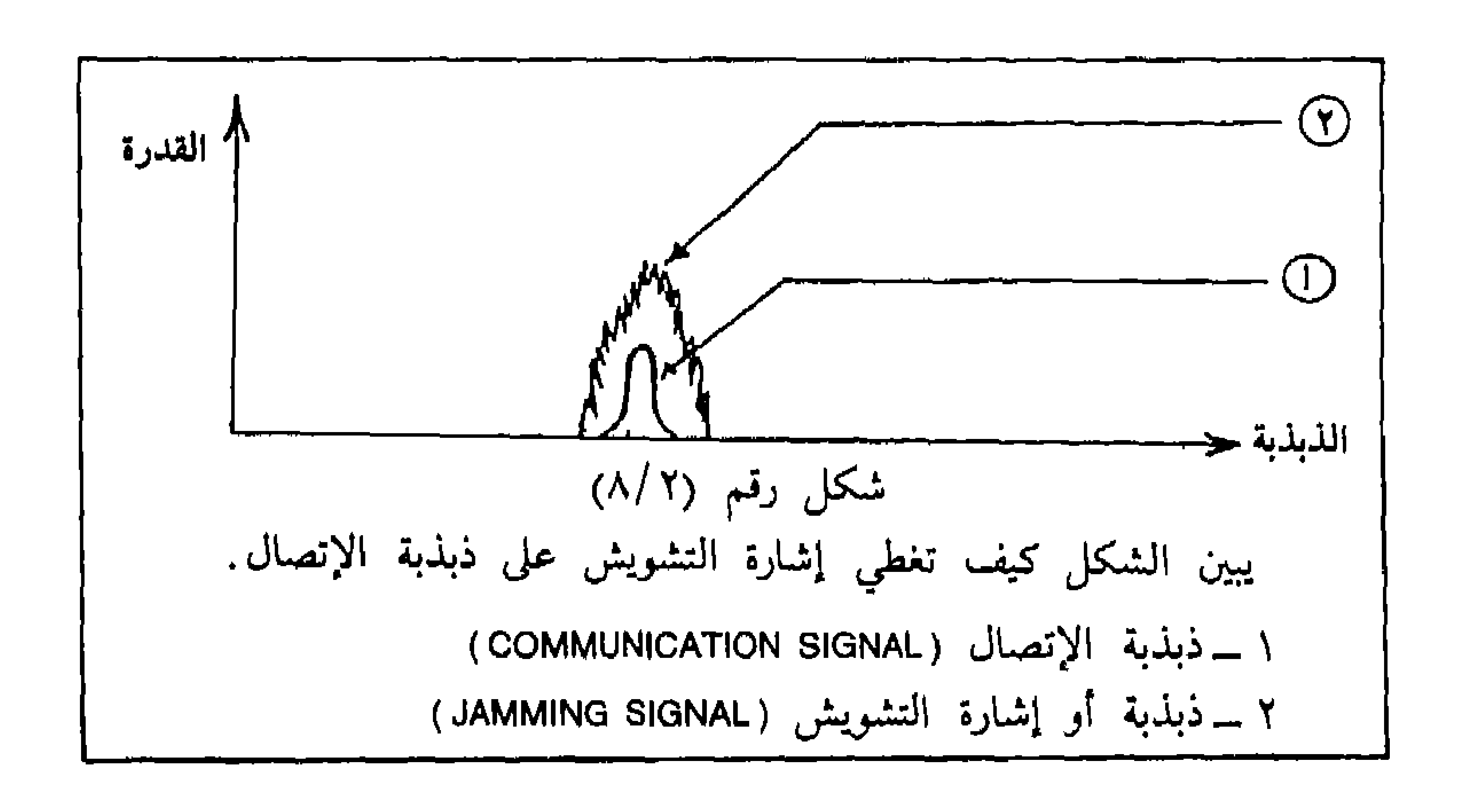
ACTIVE ELECTRONIC COUNTER MEASURES

وهي تعني التشويش بالإرسال، أي إرسال موجات ذات طاقة كبيرة إلى أجهزة العدو المستقبلة (RECEIVERS) لتحميلها أكثر من طاقتها أو بإرسال موجات ذات طاقة محدودة لمخادعتها ووضعها في حالة من الإرباك، فمثلاً لو كان هناك موقع يخاطب مركز قيادته بالراديو لبعد المسافة بينهما، وفجأة يسمع كل منهما صوتا عاليا غير مفهوم تطغي عليه الضوضاء والضجيج فلا يبلغ صوت أحد الطرفين مسامع الطرف الآخر وهذه حالة تفقد القيادة صفتها القيادية، كما تفقدها السيطرة على الأمور انظر شكل رقم (٢/٨).

أما بالنسبة للمشوش فهناك أساليب وأجهزة تعطي أكبر قدر من التأثير على إتصالات العدو.

فأوقات التشويش وحالته يجب أن تكون مدروسة وإلا فلن يكون للتشويش قيمة تذكر، كما أن المشوش يجب أن يكون حذرا. فمثلا هناك صواريخ خاصة ضد التشويش إذ تلاحق الجهاز المشوش مستعملة طريقة (HOJ = HOME-ON-JAM)

وهناك أجهزة خاصة تحدد مكان المشوش مما يوجب عليه أن يكون حذرا، وأن يعرف الوقت المناسب لتشغيل الجهاز المشوش، والوقت المناسبة لإطفائه.



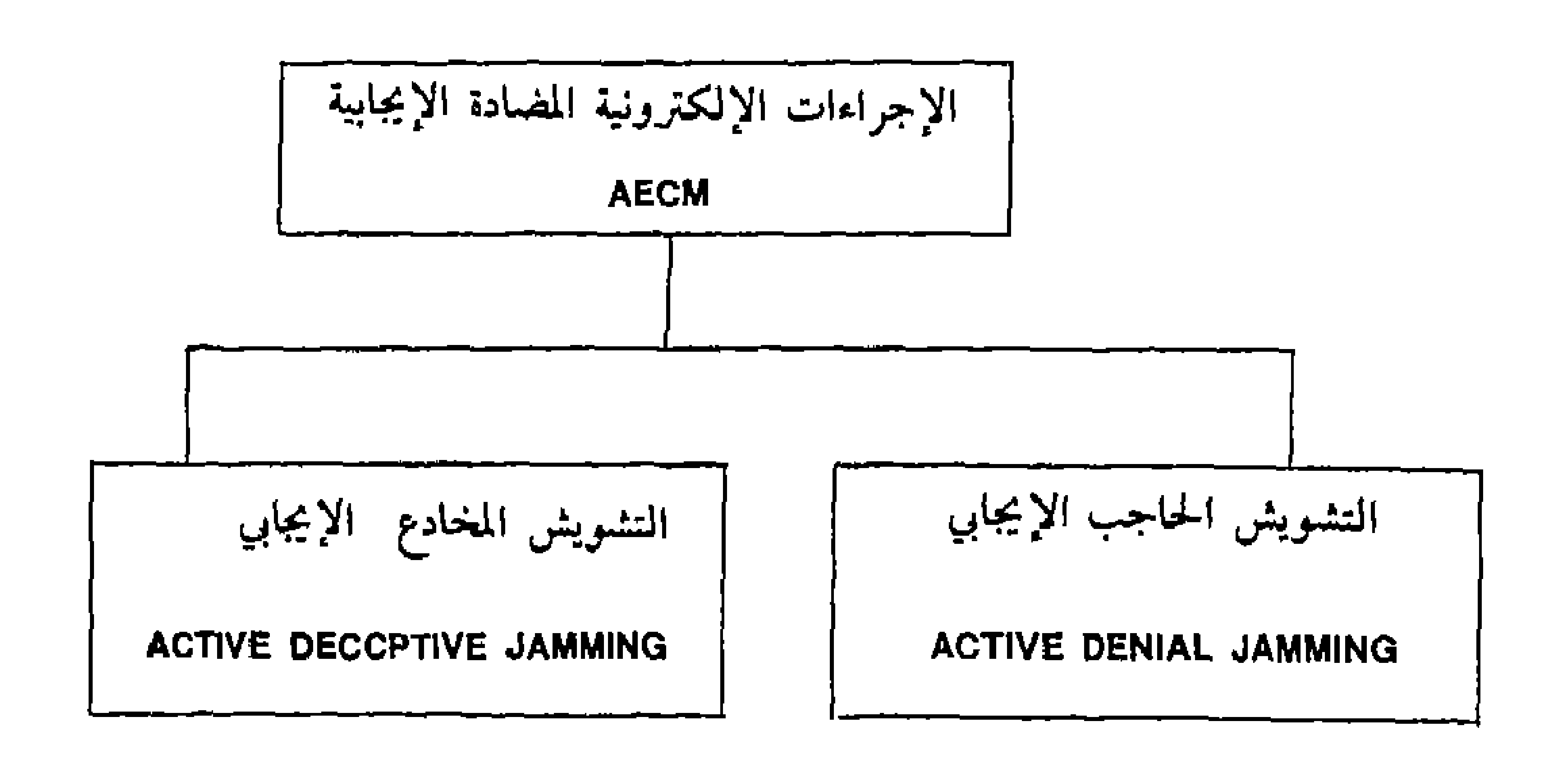
شكل رقم (٢/٨)

يبين الشكل كيف تغطي إشارة التشويش على ذبذبة الإتصال.

١ ــ ذبذبة الإتصال (COMMUNICATION SIGNAL)

٢ ــ ذبذبة أو إشارة التشويش (JAMMING SIGNAL)

وتتكون الإجراءات الإلكترونية المضادة الإيجابية (AECM=ACTIVE ELECTRO-NIC COUNTER MEASURES) من:



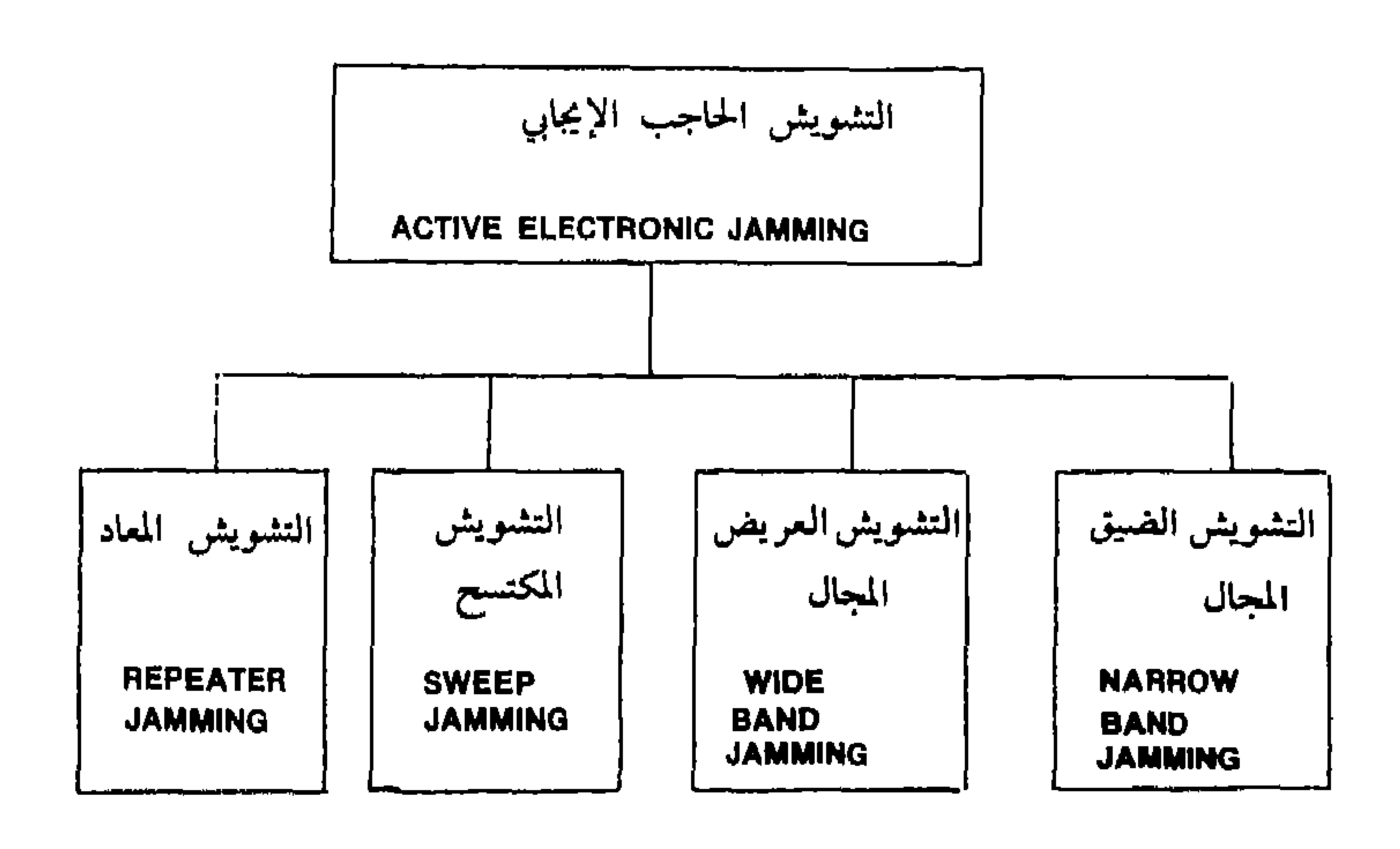
١ ـ التشويش الحاجب الإيجابي :[١] ACTIVE DENIAL JAMMING

وهو العمليات التي تستخدم فيها أساليب ومعدات تشويش إلكترونية مرسلة للتأثير على أجهزة العدو الإلكترونية المستقبلة الفعالة، لمنع أو تقليل استفادة العدو من أجهزته.

وهذا التشويش غالباً ما يكون ضجيجا (NOISE) ذو طاقة عالية يطغي على موجات وإشارات العدو بحيث لا يسمع العدو من خلال أجهزة إتصالاته سوى الضجيج العالي القدرة، أو تصبح شاشة الرادار بيضاء بفعل التشويش الضجيجي (NOISE JAMMING).

كما يطلق على التشويش الحاجب (CONCEAL JAMMING, IMPAIR JAMMING NOISE JAMMING)

ويتكون التشويش الحاجب الإيجابي من :



---

(١) ويسمى أيضاً : الضجيج الإلكتروني الإيجابي ACTIVE ELECTRONIC NOISE

أ ـ التشويش الضيق المجال : NARROW BAND JAMMING

وأيضا يطلق عليه التشويش المحدد (POINT OR SPOT JAMMING) وهو التشويش المحدد على موجة واحدة ذات مجال ضيق (± ٣,٣ كيلو هرتز للتشويش على موجه AM أو ± ١٥ كيلو هرتز للتشويش على موجة FM .. وهكذا ضد أجهزة الإتصالات) فمثلا إذا كان هناك مرسل على موجة ١٢٠ ميغا هرتز فإن جهاز التشويش يجب أن يرسل ضجيجا (NOISE) أو صفيرا مستمرا أو متقطعاً على نفس الموجه ١٢٠ ميغا هرتز، فإذا غير الأول موجته من ١٢٠ ميغا هرتز إلى ٣٥٠ ميغا هرتز مثلا فإن على المشوش إرسال تشويشه إلى ٣٥٠ ميغا هرتز، وهذا طبعا بعد المراقبة.

كما يتخلل التشويش فترات قصيرة جداً من المراقبة لمعرفة ما إذا كان هذا المرسل يبث إرساله على نفس الموجه المشوشة أم لا وكذلك التأكد من فعالية التشويش بمراقبة رد فعل العدو لأن إرسال التشويش على موجة غير مستعملة من قبل العدو لا يفيد في شيء.

ويجب أن تكون هناك دراسة لمعرفة الطاقة المناسبة للتشويش فإذا كان جهاز التشويش يرسل تشويشا بقدرة ١٥ كيلووات مثلا وكانت قدرة الطاقة كافية فلا حاجة عندئذ إلى زيادتها كما يجب أن نعرف على أي تضمين (MODULATION) يبث العدو إرساله فإذا كان يرسل على ٢٥٠ ميغا هرتز (FM) أف أم مثلا فيجب أن يكون إرسال التشويش على ٢٥٠ ميغا هرتز اف ام وهكذا إذا كان (LSB USB AM)... الخ.

في حرب ١٩٧٣ إستخدم الجيش المصري صواريخ سام ٦ لأول مرة ضد الطائرات الإسرائيلية، وكان استخدامها أمراً مفاجئاً للإسرائيليين مما أربك سلاح طيرانهم وأفقدهم الكثير من طائراتهم في بداية الحرب، لكنهم استطاعوا معرفة الموجات التي تنبعث من صواريخ سام ٦ فوضعوا أجهزة تشويش على طائرات هيلوكبتر للتشويش على رادارات تلك الصواريخ .

* أساليب التشويش الضيق المجال (أو التشويش المحدد) NARROW BAND JAMMING

هناك أساليب يجب أن تتبع من قبل المشوش لكي يحصل على تشويش مؤثر وفعال، كما أن هناك أساليب يجب أن تتبع من قبل المشوش عليه لكي يتخلص أو يقلل من أثر التشويش على أجهزته، وسنذكر فيما يلي بعض هذه الأساليب .

(١) التشويش على أجهزة الإتصالات اللاسلكية :

(أ) المركز المشوش :

عند عمل التشويش المحدد يجب أن نعرف الكثير من مواصفات أجهزة العدو حتى يكون التشويش عليه فعالا ويقلل من فائدة جهاز العدو. فمثلا يجب أن نعرف:

- الذبذبة (FREQUENCY) التي يستعملها العدو.
- التضمين (MODULATION) ... ,FM, AM, USB, LSB.
- موقع هوائي جهاز الإستقبال للعدو حتى يكون تسليط التشويش مركزاً على هذاالهوائي .
- تركيز التشويش على عُقد الإتصال (وهي مركز شبكة إتصالات العدو) .
- معرفة قدرة الإستقبال لدى العدو ولو بالتقريب حتى تكون قدرة التشويش عليه مناسبة لقدرة إستقباله ، فلا تكون قدرة التشويش أقل من المطلوب مما يجعل التشويش غير فعال، ولا تكون قدرة التشويش أكثر من المطلوب فتعتبر طاقة ضائعة، وقد تكون لها آثار جانبية.
- يجب أن تكون المسافة بين جهاز التشويش والجهاز المراد التشويش عليه مسافة مناسبة ومؤثرة .
- اختيار أرضية مناسبة (PLATFORM) لجهاز التشويش مثل طائرة أو سفينة حربية أو آلية عسكرية حتى لا يكون تدمير هذا المشوش سريعا وسهلا وبذلك نحتفظ بقدرتنا على تعمية اتصالات العدو، ويفضل أن يكون جهاز التشويش دائم التنقل.

(ب)المركز المشوش عليه :

ستختلف نتائج التشويش على جهاز الإتصال بإختلاف عوامل كثيرة منها نوعية جهاز التشويش وكفاءته ونوعية الجهاز المشوش عليه، أحوال الطقس، نوعية هوائي الجهاز المشوش عليه. . . الخ.

وسنذكر هنا بعض الصور التي يكون عليها التشويش:

- يسمع التشويش أو الضجيج على هيئة صوت محرك سيارة أو طائرة ويسمى هذا النوع بـ (NOISE JAMMING) وهذا النوع دائما يطغي على الإستقبال بحيث لا يسمع غيره، وهو أكثر أنواع التشويش إستخداماً .

ـ يسمع التشويش على شكل نغمة (TONE) أو صفير حاد أو مضخم، متقطع أو مستمر، بطيء أو سريع، وهذا النوع دائما يسمع بشكل مزعج ويسبب المضايقة والضجر وأحيانا يكون على شكل موسيقى أو صراخ أو تصفيق أو ضحك. . . الخ.

وهناك أساليب إذا ما اتبعت يكون من شأنها التخلص من التشويش أو على الأقل التقليل من فعاليته،

وفيما يلي بعض هذه الأساليب (ECCM)[1]:

ـ تغيير الذبذبة إلى أخرى أو تغيير المجال ككل وهذا التغيير يجب أن يكون متفقا عليه مسبقا مع كلا طرفي الإتصال.

ـ استخدام هوائي موجه (DIRECTIONAL ANTENNA) للإتصالات، هذا من شأنه أن يقلل من تأثير التشويش خاصة إذا كان جهاز التشويش يرسل في خط مختلف عن خط جهازي الإرسال والإستقبال.

ـ استعمال جهاز (HOPPING FREQ) وهو جهاز ينتقل من موجه إلى أخرى بصورة سريعة.

ـ إعلام مركز القيادة فورا وبدون تأخير ولفت انتباههم إلى أن التشويش المسموع تشويش ضيق المجال.

(٢) التشويش على أجهزة الرادار :

(أ) المركز المشوش :

يجب معرفة مواصفات رادار العدو لكي يكون التشويش مؤثرا عليه :

ـ معرفة الذبذبة.

ـ معرفة أنواع الإرسال مثل (PULSE OR CW).

ـ معرفة قطبية هوائي الرادار (POLARIZATION).

ـ معرفة موقع هوائي الرادار.

ـ معرفة قدرة إرسال واستقبال الرادار.

ـ إختيار المشوش المناسب على أن يكون صعب التدمير من طائرات أو سفينة حربية أو آلية ويفضل أن يكون دائم التنقل.

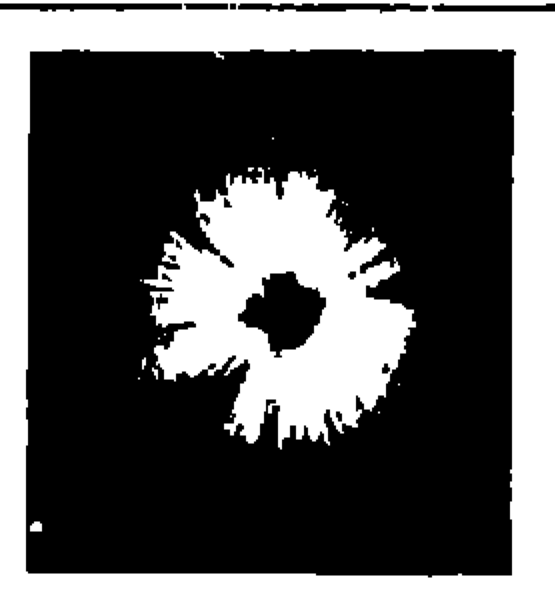
---

(١) انظر (الأساس الرابع).

(ب) المركز المشوش عليه :

عندما يحدث التشويش على الرادار، ستظهر على شاشة الرادار المشاهدات التالية :

ـ تكون شاشة الرادار كلها أو معظمها بيضاء. انظر شكل رقم (٢/٩).

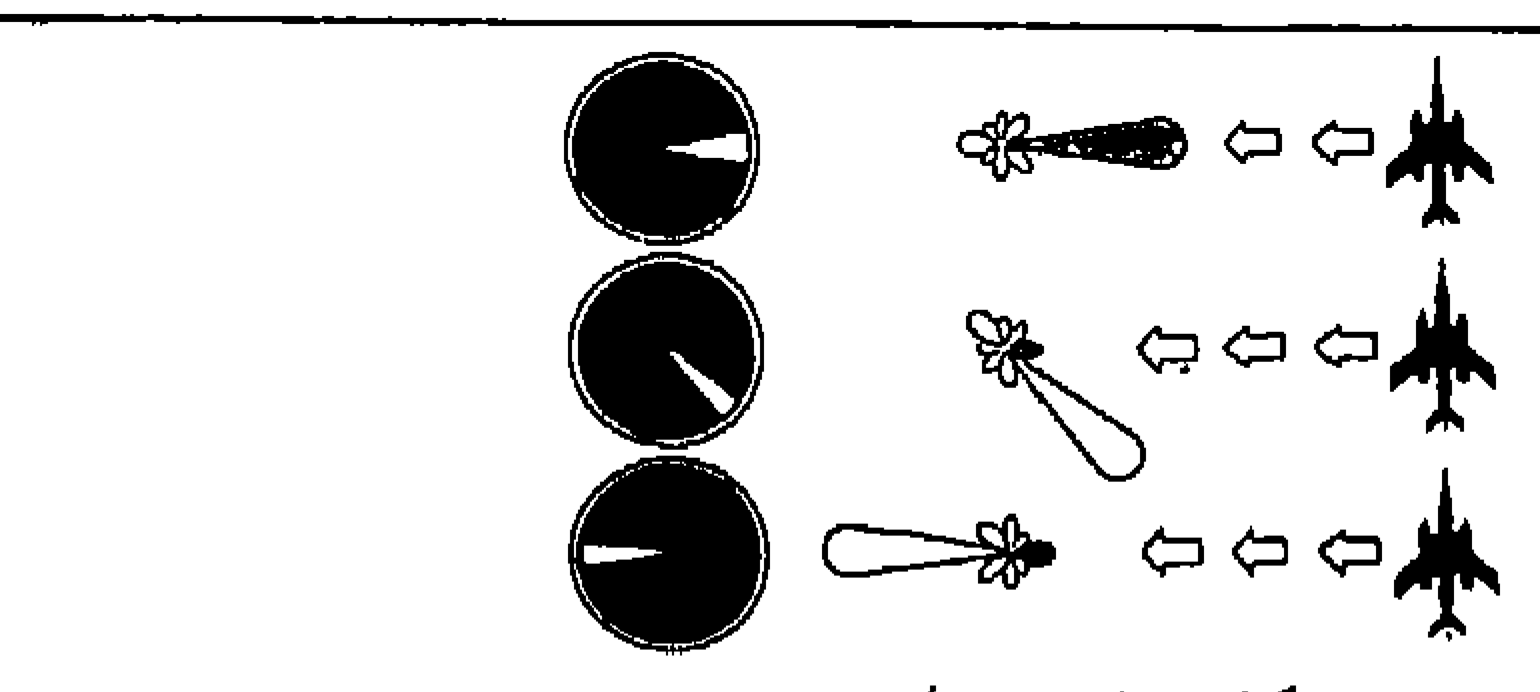


شكل رقم (٢/٩)

يبين الشكل صورة لشاشة رادار، والبياض في الشاشة قد حجب جميع الأهداف وهو نتيجة حدوث تشويش ضجيجي عالي القدرة على الرادار .

(HIGH POWER NOISE JAMMING)

ـ يكون جزء أو قطاع محدد من شاشة الرادار أبيض أو يظهر على الشاشة خط عريض أبيض ناتج عن التشـويش ، وليس بالضـرورة أن يدل هـذا الخط على إتجاه جهاز التشويش انظر شكل رقم (٢/١٠) .



شكل رقم (٢/١٠)

يظهر التشويش هنا بشكل جزئي على شاشة الرادار

الإجراءات التي يجب أن تتبع للتخلص أو التقليل من هذا النوع من التشويش (ECCM)

ـ تغيير الذبذبة أو الموجة إلى ذبذبة أو موجة أخرى ويفضل أن يتم التغيير إلى موجة أو

ذبذبة أعلى من الأولى[1].

- إستعمال جهاز التنقل السريع لذبذبة الرادار (FREQUENCY AGILITY) وهي الإنتقال السريع لعدد من الذبذبات المحددة.
- للتخلص من التشويش على الإشعاع الجانبي للرادار يستعمل (SIDE LOBE CANCLERS).
- استخدام (PULSE COMPRISION) للتقليل من تأثير التشويش على الرادار إن أمكن[2].

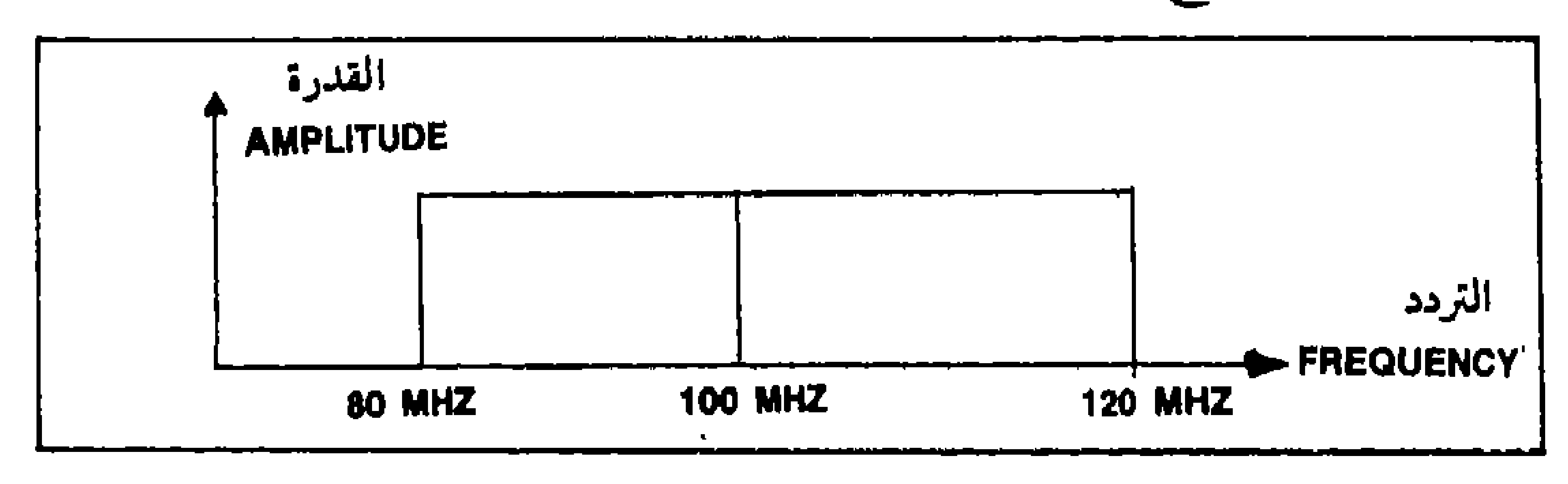
ويجب إعلام مركز القيادة فورا وبدون تأخير ولفت انتباههم إلى أن هذا التشويش محدد..

ب ـ التشويش العريض المجال: WIDE BAND JAMMING

ويقصد به التشويش أو الضجيج (NOISE) المحمول على ذبذبة معينة، وهذا الضجيج ذو مجال عريض قد يصل إلى عشرات الملايين من الهيرتز فيغطي هذا التشويش عددا كبيرا من الذبذبات والموجات.

فإذا كانت الذبذبة الحاملة (CARRIER FREQUENCY) هي ١٠٠ ميغا هرتز وعرض مجال (BANDWIDTH) = BW التشويش (الضجيج) ٤٠ ميغا هرتز (أي ± ٢٠ ميغا هرتز) فإن أي تردد أو ذبذبة تصبح بين المجال:

٨٠ ميغا هرتز و١٢٠ ميغا هرتز، ويكون مشوشاً عليه بحيث لا يسمع عند الإتصال غير الضجيج.



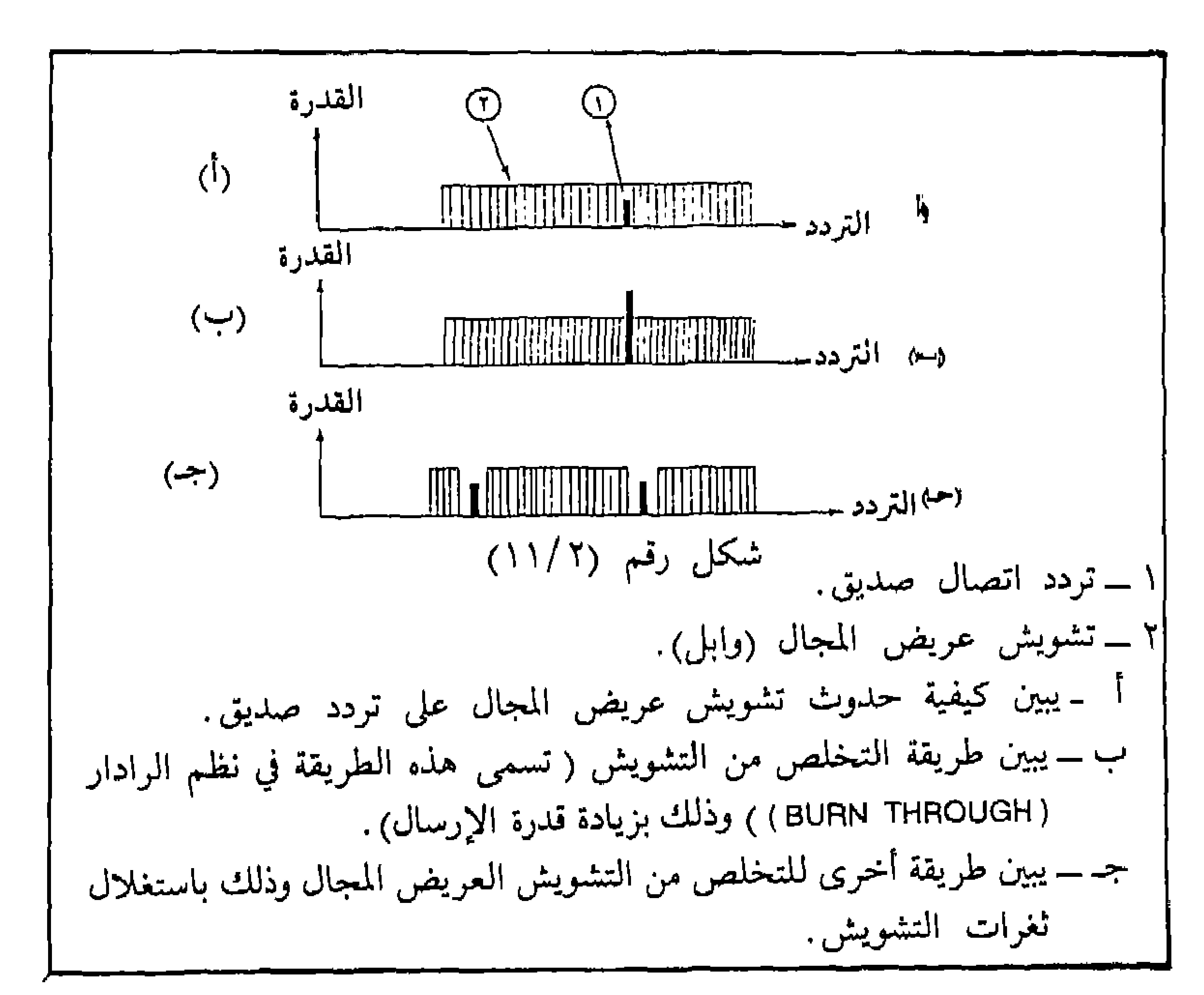
(١) انظر كتاب INTRODUCTION TO RADAR SYSTEM صفحة ٥٤٧.
(٢) المصدر السابق.

وقد يصل عرض المجال (B.W) إلى أكثر من هذا، فقد يصل إلى ± ١٠٠ ميغا هرتز حسب نوعية جهاز التشويش.

وعادة يستعمل هذا النوع من التشويش في حالة التوتر الشديد أو الحرب وفي الهجوم خاصة، فيسلط هذا التشويش مثلا على المنطقة المراد الهجوم عليها لتعمية راداراتها أو إتصالاتها وهذا من شأنه التقليل من فعالية القوات المراد الهجوم عليها.

وهذا النوع من التشويش يسهل كشفه ومعرفته بأنه تشويش عريض المجال، فإذا صادفنا هذا التشويش على ذبذبة أو تردد ما، وغيرنـا هذا الـتردد إلى تردد أعـلى أو أدنى، بصورة سريعة ولاحظنا أن النتيجة لم تتغير أمكننا التأكد من أنه تشويش عريض المجال.

والتشويش العريض المجال يطلق عليه أيضا: التشويش الوابل (BARRAG JAMMING) أو التشويش السد، أو التشويش الحاجز. انظر شكل (١١/٢).



شكل رقم (١١/٢)

١ ـ تردد اتصال صديق.

٢ ـ تشويش عريض المجال (وابل).

أ - يبين كيفية حدوث تشويش عريض المجال على تردد صديق.

ب ـ يبين طريقة التخلص من التشويش (تسمى هذه الطريقة في نظم الرادار (BURN THROUGH)) وذلك بزيادة قدرة الإرسال).

جـ ـ يبين طريقة أخرى للتخلص من التشويش العريض المجال وذلك باستغلال ثغرات التشويش.

وكما رأينا في التشويش الضيق المجال ومضاداته، سنبين هنا مضادات التشويش عريض المجال.

(١) في مركز الإتصالات المشوش عليه بتشويش عريض المجال.

هناك إجراءات يجب أن يتبعها هذا المركز للتخلص أو التقليل من تأثير هذا النوع من التشويش باستخدام المضادات (ECCM) ومنها :

- تغيير الذبذبة من مجال إلى آخر (..HF, VHF, UHF).
- زيادة قدرة الإرسال.

لأن من عيوب هذا النوع من التشويش قلة قدرة التشويش على تغطية مجال التشويش بالكامل بكفاءة عالية.

- استخدام هوائي موجه (DIRECTIONAL ANTENNA) للإتصالات، هذا من شأنه أن يقلل من تأثير التشويش خاصة إذا كان جهاز التشويش يرسل في غير خط جهاز الإرسال والإستقبال.
- إستعمال جهاز (SPECTRUM ANALYSER) : إذ بهذا الجهاز يمكن معرفة ما إذا كانت هناك ذبذبات لم يشوش عليها ضمن المجال المشوش عليه انظر شكل رقم (٢/١١).
ويكون التشويش على قسمين أو ثلاثة أو أكثر لتغطية المجال العريض وعلى سبيل المثال يكون التشويش على الذبذبات:
في مجال (VHF) من ٣٠ إلى ٨٥ ميغا هرتز، ومن ٩٠ إلى ١٥٠ ميغا هرتز فيكون الإتصال متاحاً في الذبذبات من ٨٥ إلى ٩٠ ميغا هرتز .
- إعلام مركز القيادة فوراً وبدون تأخير لافتاً إنتباههم إلى أن هذا التشويش عريض المجال.

(٢) الرادار المشوش عليه بتشويش عريض المجال :

هناك إجراءات يجب أن تتبع للتخلص أو التقليل من تأثير هذا النوع من التشويش (ECCM) ومنها :

- تغيير الذبذبة من مجال إلى آخر، أو استخدام ذبذبات بعيدة جدا عن الذبذبة السابقة في نفس المجال (التغيير من ٢٥٠٠ ميجا هرتز إلى ٥٥٠٠ ميجا هرتز إن أمكن).

ـ زيادة قدرة ارسال الرادار بإتجاه المشوش ليكون صدى الرادار أكبر من قدرة جهـاز التشويش ، وهذه الطريقة تسمى (BURNTHROUGH)[1] .

ـ إذا كان هناك رادار يتكون من جزئين : رادار كشف (SURVEILLANCE RADAR) ورادار موجد الإرتفاع (HEIGHT FINDER RADAR)
فالأفضل أن يستعمل كل رادار ذبذبة بعيدة عن ذبذبة الرادار الثاني، أو في مجال آخر حتى إذا شوش على أحدهم يستطيع الآخر تحديد موقع الأهداف إذ من الصعب التشويش على مجالين في وقت واحد، وتسمى هذه الطريقة (FREQUENCY DIVERSITY).
ـ إستعمال رادار ذي هوائيين إثنين وشاشة واحدة، يستعمل مجالين للذبذبات في وقت واحد فإذا شوش عل أحدهما يستمر الثاني في العمل.
وإعلام مركز القيادة فوراً وبدون تأخير لافتا إنتباههم إلى أن هذا التشويش (تشويش عريض المجال).

ولهذا النوع من التشويش عيوب منها :

١ ـ يحتاج إلى قوة إرسال كبيرة جداً ليكون تشويشه فعالا ومغطيا كل مجال التشويش.

٢ ـ إحتمال التشويش على الأجهزة الصديقة التي تستعمل ذبذبات في نفس مجال التشويش.

٣ ـ صعوبة الحصول على هوائي مثالي لهذا النوع من أجهزة التشويش، وهذا يؤدي إلى وجود (HARMONICS) تؤدي بالتالي إلى تقليل قدرة التشويش وتزيد من احتمال التشويش على أجهزة صديقة أخرى.

جـ ـ التشويش المكتسح : SWEEP JAMMING

وهو تشويش يجمع بين صفتي التشويش الضيق المجال والتشويش العريض المجال، فهو تشويش يكون على شكل ذبذبة حاملة مجالا ضيقا من الضجيج (NOISE)

---

(١) كتاب INTRODUCTION TO RADAR SYSTEM صفحة ٥٤٧.

لكنها لا تكون ثابتة فهي تتحرك بإتجاه واحد إما أعلى أو أدنى كاسحة عدة ذبذبات بالتشويش عليها، فهي تبدأ من ذبذبة ١٠٠ ميغا هرتز متجهة إلى أعلى حتى ذبذبة ١٥٠ ميغا هرتز مثلا، ثم ترجع كاسحة في رحلة الإياب حتى ذبذبة ١٠٠ ميغا هرتز وهكذا كالمنشار، فيغطي التشويش بهذه الطريقة عدد كبيرا من الذبذبات (٥٠ ميغا هرتز عرض مجال التشويش).

وطريقة المنشار هذه طريقة قديمة لهذا النوع من التشويش، أما الآن فتستخدم طريقة الذهاب فقط وليس الذهاب والإياب، أي من ١٠٠ ميغا هرتز إلى ١٥٠ ميغا هرتز ثم تبدأ مرة ثانية من ١٠٠ ميغا هرتز إلى ١٥٠ ميغا هرتز وهكذا باتجاه واحد في نفس المجال.

وعادة ما يكون جهاز التشويش هذا مستخدماً جهاز كمبيوتر لتكون عمليات التشويش أكثر تنظيما وكلما كان الإكتساح أو المسح سريعا كان التشويش ذا فعالية أكبر وتأثير أقوى.

والتشويش المكتسح يطلق عليه أيضا: التشويش بالمسح أو التشويش المنزلق.

د ـ التشويش المعاد: REPEATER JAMMING

يجمع هذا النوع من التشويش أيضا بين صفتي التشويش الضيق المجال والتشويش العريض المجال، فهو تشويش يكون على شكل ذبذبة حاملة مجالا ضيقا من الضجيج (NOISE)، ويحدث الإرسال (التشويش) فقط عند استقبال ذبذبة العدو، فإذا كان مجال جهاز التشويش هذا من ١٠٠ ميغا هرتز إلى ٢٠٠ ميغا هرتز مثلاً، يكون الإرسال أو التشويش في حالة صمت (أي بدون إرسال) فإذا التقطنا إرسال العدو على هذا المجال (من ١٠٠ ـ ٢٠٠ ميغا هرتز) يقوم الجهاز تلقائيا بإرسال تشويشه على ذبذبة العدو، فإذا أرسل على ١٦٠ ميغا هرتز يشوش فقط على ذبذبة ١٦٠ ميغا هرتز، وإذا أرسل العدو على ذبذبة ١٠٥ ميغا هرتز يرسل الجهاز تشويشه فقط على ١٠٥ ميغا هرتز وهكذا.

وعادة يكون التشويش المعاد الراداري على أجهزة الرادار المعادية التي تعمل (LOCK-ON) وتعني تسليط الأشعة الرادارية على الهدف فيقوم بالتشويش على رادار

(١) المصدر السابق.

العدو. لذا فالتشويش المعاد يستعمل للتشويش على الرادارات المستخدمة نظام تنقل الذبذبات (FREQ. AGILITY RADAR) وعادة يسمى التشويش المعاد على أجهزة الإتصالات بالتشويش التابع (FOLLOWER JAMMING) وهو عادة يستخدم للتشويش على الإتصالات التي تتبع طريقة تغيير الذبذبة» انظر شكل رقم (٢/١٢).

القدرة (١)	(٢)	(٣)	التردد (٤)
* محاسن هذا التشويش : - كفاءة عالية. - الجهاز صغير الحجم وبسيط. - عدم التأثير على ذبذبات أخرى.	* محاسن التشويش : - لا يحتاج كفاءة عالية للتشغيل - يغطي مجال عريض في نفس الوقت	* محاسن التشويش: - لا يحتاج إلى كفاءة عالية للتفشيل. - كفاءة عالية للتشويش	* محاسن التشويش: سهولة الاستعمال
* مساوىء هذا التشويش : - يحتاج مشغل وجهاز عال الكفاءة لتحديد الذبذبة المراد التشويش عليها.	* مساوىء التشويش : - يحتاج طاقة تشويش كبيرة - التشويش ليس عالي الكفاءة - احتمالية التشويش على صديق.	* مساوىء التشويش : - سهولة خداعه وذلك بارسال موجات غير ذات أهمية	* مساوىء التشويش : - احتمالية التشويش على صديق - قليل الكفاءة إذا كان المجال عريض جداً.

شكل رقم (٢/١٢)

يبين أنواع التشوش الإلكتروني الإيجابي.

أ ــ الذبذبات المراد التشويش عليها.

ب ــ ذبذبات التشويش

١ ــ التشويش الضيق المحال: التشويش على ذبذبة واحدة بمجال ضيق.

٢ ــ التشويش العريض المجال: التشويش على مجال كامل لجميع الذبذبات المتواجدة فيه.

٣ ــ التشويش المعاد: التشويش على فقط الذبذبات الموجودة في هذا المحال.

٤ ــ التشويش المكتسح: يبدأ التشويش على أول ذبذبة ثم يتجه للتشويش على الذبذبات الأخرى، مكتسحا جميع الذبذبات في ذلك المجال ،ثم يعود مرة ثانية مشوشا بنفس الطريقة وهكذا بحركة سريعة.

٢ ـ التشويش المخادع الإيجابي : ACTIVE ELECTRONIC DECEPTION

وهي العمليات التي تستخدم فيها أساليب ومعدات تشويش الكترونية مرسلة لتضليل أجهزة العدو الإلكترونية المستقبلة الفعالة.

وهو تشويش له خاصية مخادعة وتضليل إتصالات العدو وراداراته فهو يعتمد على طريقة التداخل في موجات العدو وإعطائه معلومات خاطئة ليتخذ خطوات تكون بالتالي خاطئة، أو لخداع رادار العدو بإعطائه أهدافاً غير صحيحة كماً وحجماً، بعداً وقرباً (مسافة أو مدى).

وهذا النوع من التشويش يجب فيه المعرفة والمراقبة التامة بشبكة إتصالات العدو وشبكة راداراته أو أجهزته الأخرى، حتى إذا قمت بالتشويش المخادع عليه بإرسال أهداف وهمية أو معلومات غير صحيحة تنطلي عليه هذه الخدعة، ونجاح التشويش هنا يكمن في رد فعل العدو الخاطىء لأنه أصلا معتمد على معلومات خاطئة.

ويكتمل النجاح عند استغلال إجراءات العدو الخاطئة الناتجة عن التشويش المخادع، لمهاجمته مثلا أو ضرب معداته أو طائراته الحربية.. الخ.

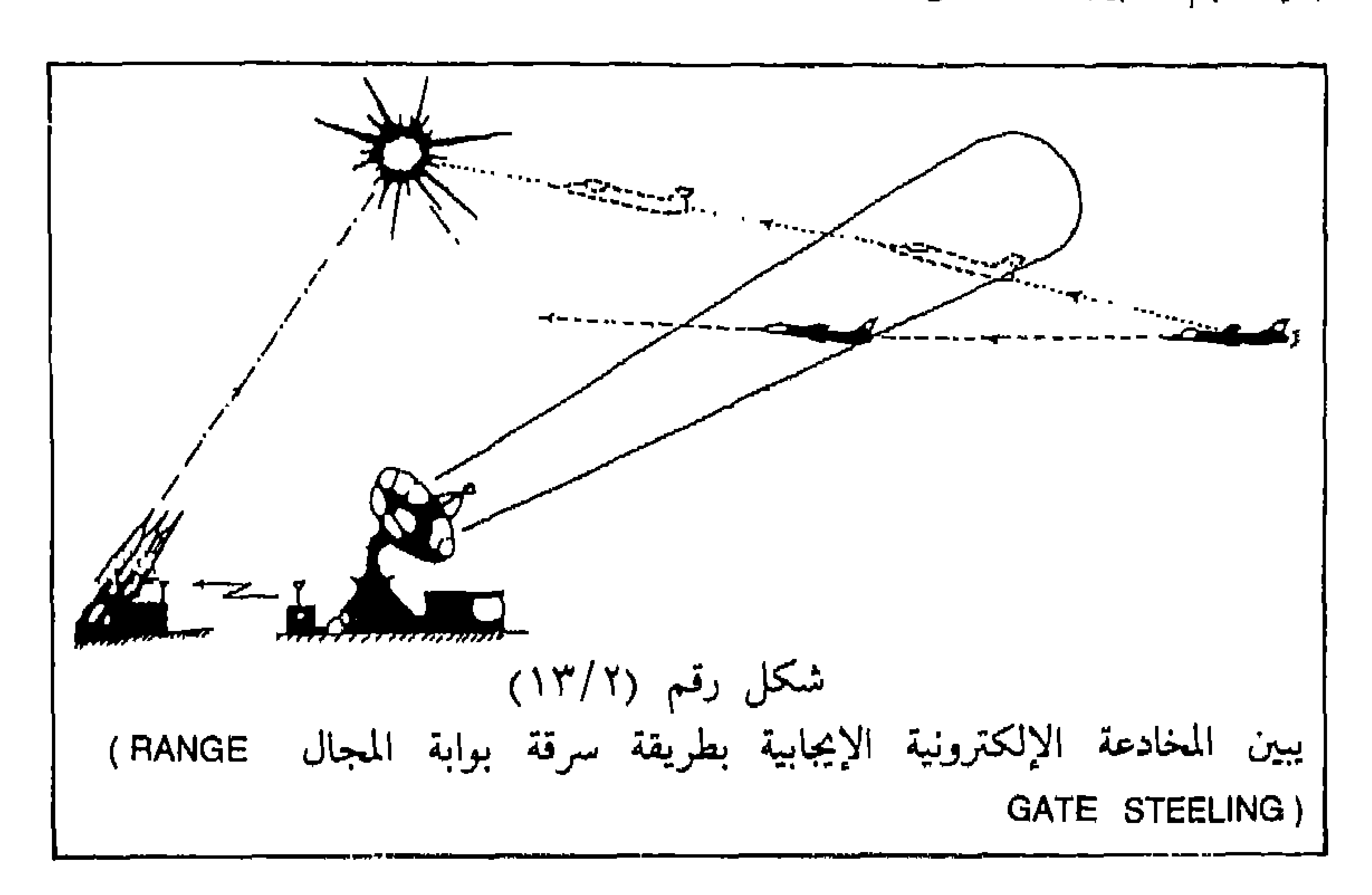
وهناك طريقة أخرى لخداع العدو هي إعطاؤه معلومات بطريق غير مباشر على أن يكون القليل من هذه المعلومات صحيحا والباقي خطأ، ويجب أن تكون هذه المعلومات من الكثرة بحيث تجعل العدو مثقلا (OVER LOADED) لأن كمية المعلومات الهائلة ستشغله وقتا طويلا في تحليلها وتفنيدها مما يعطي المشوش فرصة الإستفادة الكاملة من وقت العدو وجهده الضائعين.

وثمة طريقة أخرى للتشويش المخادع تسمى (MANIPULATIVE JAMMING) فعندما نتأكد من أن العدو يتصنت على ذبذبتنا يقوم فريقان ـ بالإستعانة ـ بأجهزة إتصالات لاسلكية ـ تبادل المحادثة، بحيث تحتوي على القليل من الصواب والكثير من الخطأ، حتى يتم تضليل العدو فيتخذ على أساسها إجراءات خاطئة.

أو بتسجيل محادثة للعدو عبر أجهزة إتصالاته وبعد فترة زمنية يتم الإتصال به ونسمعه تسجيل صوت الطرف الآخر محرفا وتسمى هذه الطريقة باسم (IMITATIVE DECEPTION).

وسنذكر طريقة أخرى من طرق التشويش المخادع حتى نقرب الفكرة إلى الذهن وهي طريقة تعرف باسم (R.G.C. = RANGE GATE CAPTURE[1]) أو «سرقة بوابة المجال» (R.G.S: RANGE GATE STEELING) وذلك باستخدام جهاز التشويش المعاد (REPEATER JAMMER)

وكما هي مبينة في الشكل (١٣/٢) فعندما تلتقط الطائرة المشوشة إرسال الرادار الأرضي، وكما نعلم فإن الرادار يكشف الهدف عن طريق إرسال موجة على شكل (PULSE) ثم يستقبل هذه الموجة عند اصطدامها بهدف ويحسب الوقت ما بين الإرسال والإستقبال ليبين لنا مدى الهدف.



شكل رقم (١٣/٢)
يبين المخادعة الإلكترونية الإيجابية بطريقة سرقة بوابة المجال (RANGE GATE STEELING)

يقوم جهاز التشويش الموجود بالطائرة بإعادة إرسال الموجة بطاقة أكبر قليلاً، ولكي يحقق المخادعة فإنه يجعل الإعادة إما متأخرة أو متقدمة فيبين لنا الرادار الأرضي للمدفعية أن الهدف الآن إما قريب جداً وإما بعيد جداً، وبالتالي يكون التصويب خاطئاً نتيجة المخادعة، ويكون الموقع الأرضي لقمة سائغة للطائرات المهاجمة .

(١) يقصد بـ RANGE GATE هي عملية من عمليات أجهزة الرادار الداخلية لتحديد بُعد هدف معين وذلك بعد تحديد إتجاهه.

ومن الطرق المضادة لهذا التشويش إستعمال المدفع أرض ـ جو إستعمالا يدوياً (MANUAL CONTROL) إذ يمكن بالعين المجردة التحكم بإطلاق المدفع على الأهداف. وطبعا هذه طريقة واحدة فقط من الطرق المتعددة لمضادات التشويش المخادع وقد استخدمت فعلا في حرب ١٩٧٣ من قبل القوات المسلحة المصرية عندما أراد الإسرائيليون التشويش على رادار المدافع المضادة للطائرات، وهي من نوع (SHILKA).

أساليب التشويش المخادع :

هناك أساليب يجب أن تتبع من قبل المشوش لكي تنطلي الخدعة على المشوش عليه، كما أن هناك أساليب يمكن أن يتبعها المشوش عليه ليتأكد من أنه تشويش مخادع ويتخلص منه ، وسنذكر هنا بعض الأساليب :

أ ـ المركز المشوش :

سبق أن تحدثنا عما يجب على المركز المشوش إتباعه ليكون التشويش مؤثرا، والمعلومات نفسها يجب على المركز المشوش معرفتها عند عمل التشويش المخادع، مع توفر الدقة فيها من حيث الذبذبة والتضمين وقدرة إستقبال الجهاز المراد التشويش عليه . . . الخ .

وكذلك هنا يجب معرفة بعض المعلومات والأسرار التي يساعد إستخدامها على التشويش المخادع. هذا بالنسبة لأجهزة الإتصالات. أما بالنسبة لأجهزة الرادار فلابد من معرفة بعض المواصفات الدقيقة للرادار المراد التشويش عليه كخواص ومدى الأشعة الرئيسية (MAIN LOBE) والجانبية للرادار والتي تسمى الوريقات الجانبية (SIDE LOBES) لكي يكون التشويش المخادع من الجهتين أو من إحداهما ، كذلك معرفة كيفية عمل الرادار إذا كان رادار تتبع . . . إلخ .

ب ـ المركز المشوش عليه :

(١) أجهزة الإتصال اللاسلكي :

من تأثير التشويش المخادع على أجهزة الإتصال سنلاحظ مثلا :

ـ استقبال معلومات أو أوامر محيرة بعض الشيء أو غير متوقعة.

ــ استقبال كم هائل من المعلومات عن أشياء عديدة تؤدي إلى الملل والضجر.
ــ استقبال معلومات أو أوامر مؤسفة وأخبار غير سارة عن المواقع الأخرى أو عن تـدمير بعض القوات الصديقة.

إذا لاحظنا مثل هذه المعلومات وأدركنا أنها نتيجة تشويش مخادع فهناك إجراءات يجب أن تتبع للتخلص من هذا النوع من التشويش أو تقليل فعاليته (ECCM) مثل :

ــ التغيير إلى ذبذبة متفق عيها بين طرفي الإتصال لم تستعمل مطلقا من قبل إنما كانت موضوعه للحالات الطارئة.
ــ استخدام كلام مشفر متفق عليه سابقا، أو رموز تعريف محطات الإتصال.
ــ الأفضل استعمال أجهزة تشفير إلكترونية عالية الكفاءة ومتطورة.
ــ إعلام مركز القيادة على الفور، ولفت إنتباههم إلى أن هذا التشويش تشويش مخادع.

(٢) أجهزة الرادار :

ينتج عن التشويش المخادع على أجهزة الرادار ما يلي :

ــ تظهر على شاشة الرادار معلومات غير صحيحة ومتغيرة ومحيرة عن حجم الهدف، سرعة الهدف، بعد الهدف.

وعادة تكون هذه المعلومات سريعة التغير فمثلا أن يكون الهدف بعده حوالي ٩٥كم وفجأة وبعد لحظات معدودة يكون على بعد ١٥ كم.

ــ عدد الأهداف تتكاثر وتتناقص بسرعة عجيبة وبصورة مفاجئة.

إذا حصل مثل هذا فهناك إجراءات يجب أن تتبع، إذ أن من شأنها التخلص من هذا النوع من التشويش أو تقليل التأثير على شاشة الرادار (ECCM) منها:

ــ تغيير ذبذبة الرادار فجأة من ذبذبة إلى أخرى قريبة أو بعيدة.
ــ تغيير أوقات النبضة (PRF JETTERING) .
ــ استخدام نظام (FREQUENCY AGILITY).
ــ استخدام (SIDE LOBE CANCELLER AND SIDE LOBE BLANKER) للتخلص من التشويش المخادع على الأشعة الجانبية أو الوريقات الجانبية (SIDE LOBES).
ــ تغيير قطبية هوائي الرادار.
.وإعلام مركز القيادة فورا، ولفت انتباههم إلى أن هذا التشويش «تشويش مخادع».

وعموما هناك بعض المساوىء لأجهزة التشويش (JAMMERS) ومنها:

١ ـ إضاعة المفاجأة التكتيكية: (LOSS OF TACTICAL SURPRISE)

إذ يدل التشويش على أن هناك أفرادا أو قوات موجودة تقوم بالتشويش وهذا من شأنه إذا استعمل من البداية إضاعة فرصة المفاجـأة التكيتيكة ضد العدو.

٢ ـ الوضوح: إذ أن جهاز التشويش بسبب قوة إرساله سوف يكون صيدا سهلا لأجهزة المراقبة المعادية (ESM) وكذلك لموجد الإتجاه (DF-DIRECTION FINDERS) الذي يحدد موقعه.

٣ ـ التداخل: إذ أن التشويش يسبب أحيانا بعض التأثيرات على الأجهزة الإلكترونية الصديقة.

ب ـ الإجراءات الإلكترونية المضادة السلبية :
PASSIVE ELECTRONIC COUNTER MEASURES (PECM)

وهي « العمليات التي تستخدم فيها أساليب ومعدات عاكسة للتأثير أو لمخادعة أجهزة العدو الإلكترونية الفعالة لتقليل استفادته منها ».

وتعمل هذه المعدات العاكسة (REFLECTORS) على عكس الموجات الكهرومغناطيسية أو تشتيتها حتى لا يستفيد منها العدو إذا استقبلها في معداته الكشفية، وحتى تحمي أو تستر منطقة معينة من مراقبة العدو وبعبارة أخرى توضع معداتنا وطائراتنا تحت خطر غير مباشر من قبل معدات العدو كراداراته مثلاً أو صواريخه .

وهذه المعدات معدات سلبية أي ليس لها إرسال أو بث كهرومغناطيسي إنما لها خاصية عكس تلك الموجات أو تشتيتها أو امتصاصها (REFLECTION, DEFLECTION, ABSORBING) ولمعدات الإجراءات الإلكترونية المضادة السلبية (PECM) خاصية التشـويش الحـاجب والتشويش المخادع حسب تصميمها.

وسنذكر هنا بعض أنواع معدات الإجراءات الإلكترونية المضادة السلبية :

أ ـ النوافذ أو النصلات(١) WINDOWS OR CHAFF

وهي تتكون من عيدان صغيرة جدا تنثر في الجو يكون طولها = نصف طول موجة الرادار المراد التشويش عليه وهي عادة تكون مصنوعة من :
أ ـ زجاج أو بلاستيك أو فيبر غلاس مطلية بألمونيوم أو حديد رفيع.
ب ـ صفائح أو شرائط معدنية رقيقة.

ولهذه العيدان الصغيرة خاصية كبيرة فهي تعكس أكبر قدر ممكن من طاقة موجات الرادار فعند قذفها تهبط ببطء وتتحرك باتجاه الريح، فتظهر كأنها أهداف متحركة ببطء فينتج عن ذلك ظهور بقع بيضاء (كأنها CLUTTER) على شاشة الرادار أو تظهر على شكل غمامة كثيفة وضباب الكتروني تحجب الهدف الحقيقي وهنا يجب معرفة سرعة الـريح حتى نحـافظ على وجـود الطائـرة داخل أو خلف الضبـاب الإلكـتروني، ويستـطيـع الـرادار التخلص بعض الشيء من هذا التـأثير بـاستخدام (MOVING TRAGET INDICATION)

---

(١) في بعض الكتب العلمية توصف بـ: MECHANICAL JAMMING

("M.T.I.") كما يجب أن نعلم أن النصلات لا تؤثر على الرادارات ذات الموجات المستمرة (C.W. RADAR) وتطلق هذه العيدان أو النصلات من الطائرة إما يدويا أو أوتوماتيكيا كما أن هناك شركة أمريكية[1] تنتج نوعا من الأجهزة التي تطلق النصلات (CHAFF) أوتوماتيكيا عندما تأتيه إشارة من جهاز الإستقبال الراداري للإنذار الموجود بالطائرة ويقوم هذا الجهاز بتقطيع هذه العيدان بأطوال تناسب طول موجة الرادار والمراد التشويش عليه وتتم هذه العملية في ثوان معدودة .

وتقذف هذه النصلات من الطائرة إما إلى الأمام أو إلى الجانب أو إلى الخلف طبقا للعمليات الهجومية أو الدفاعية .

٢ ــ الطعم أو الهدف : DECOY OR TARGET

ويقصد بالطعم أو الهدف الطائرات بدون طيار[2] صغيرة الحجم وهي عادة من نوع (DRONE) ، ولهذا النوع شكل وطلاء خاص يجعلها على صغر حجمها تعكس أكبر قدر من أشعة الرادار (وخاصة الرادار الأرضي) فتظهر على شاشته وكأنها هدف كبير الحجم .

والفرق بين الطعم والهدف، أن الطعم طائرة بدون طيار تطلق من الطائرات باتجاه الرادارات المعادية لتضليلها فتوجه أسلحة العدو من مدافع أرضية أو صواريخ نحو الطعم فتنجو بذلك الطائرة أو الهدف الحقيقي . انظر شكل رقم (٢/١٤).

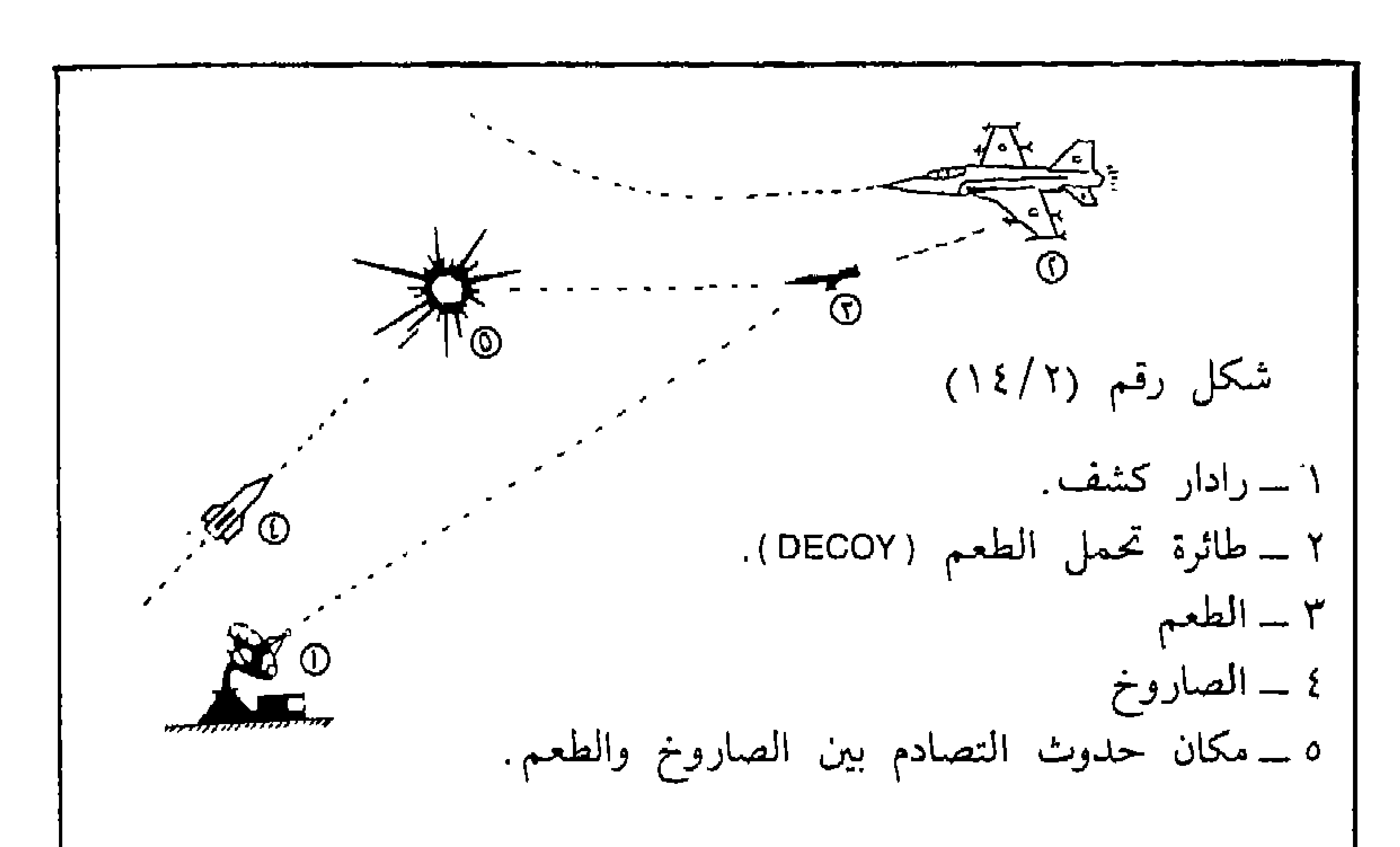
والهدف يقوم بنفس عمل الطعم إلا أنه فقط ينطلق من محطة أرضية على عكس (الطعم) الذي ينطلق من محطة جوية (طائرة) .

وكذلك باستطاعة الطعم أو الهدف الذي يعكس أقل كمية من أشعة الرادار أن يحمل معدات إلكترونية مختلفة تساعد في التضليل أو إعاقة قوات العدو، مثل أجهزة (تشويش أو مخادعة إلكترونية) ولها جهاز للتحكم عن بعد لإختراق أجواء العدو أو التغلغل في أعماقه ، وبها مواد متفجرة وقنابل لتدمير مواقع العدو عند السقوط في أراضيه .

كذلك ممكن إستخدام الركن العاكس (CORNER REFLECTOR) وهو جسم له أبعاد معينة وشكل هندسي دقيق يعكس أكبر قدر من أشعة الرادار، ليوضع في مكان معين أو أن يطلق من سفينة أو طائرة فيعتبره الرادار أو الصاروخ الموجة بأنه هدف كبير فينطلق إليه ويصيبه .

(١) شركة GOOD YEAR الأمريكية .

(٢) انظر الباب الثالث. «الطائرات بدون طيار» .



شكل رقم (١٤/٢)

١ ــ رادار كشف.
٢ ــ طائرة تحمل الطعم (DECOY).
٣ ــ الطعم
٤ ــ الصاروخ
٥ ــ مكان حدوث التصادم بين الصاروخ والطعم.

يبين الشكل عملية خداع الرادار بإطلاق الطعم نحو موقع الرادار ليكتشفه الرادار، وبعد ذلك يطلق الصاروخ لإصابة ذلك الهدف (الطعم) بدلا من الهدف الحقيقي (الطائرة) التي بذلك ستؤدي مهمتها بسلام.

٣ ــ الدخان : SMOKE

وهو من الأشياء التي تعمل على حجب أشعة الليزر حيث يشوش على أجهزة الليزر ويستر الموقع المسلط عليه تلك الأشعة التي إما أن تكون للكشف أو لقياس البعد أو لتوجيه صاروخ نحوه.

فللدخان خاصية عكس وتشتيت جميع الموجات الضوئية التي تستخدمها أجهزة أشعة الليزر، خاصة إذا كان الدخان كثيفاً.

كذلك معظم المعدات أو الأشياء التي تحجب نظر ورؤية الإنسان كالغبار والغيوم.. الخ.

٤ ــ التمويه : CAMOUFLAGE

ويقصد بالتمويه هنا استخدام أساليب أو معدات مختلفة لخداع (أو لتشويش)

معدات كشف العدو الإلكترونية وذلك بحجب أو ستر معداتنا ومواقعنا من أن تكتشفها معدات العدو الكشفية.

كذلك من طرق ونظم الإجراءات الإلكترونية المضادة السلبية الحديثة وخاصة في الطيران تصميم الطائرة بطريقة تقلل من قوة كشف رادار العدو لها، ويسمى هذا تقنية الإختفاء (STEALTH TECHNOLOGY) ومن خصائصه :

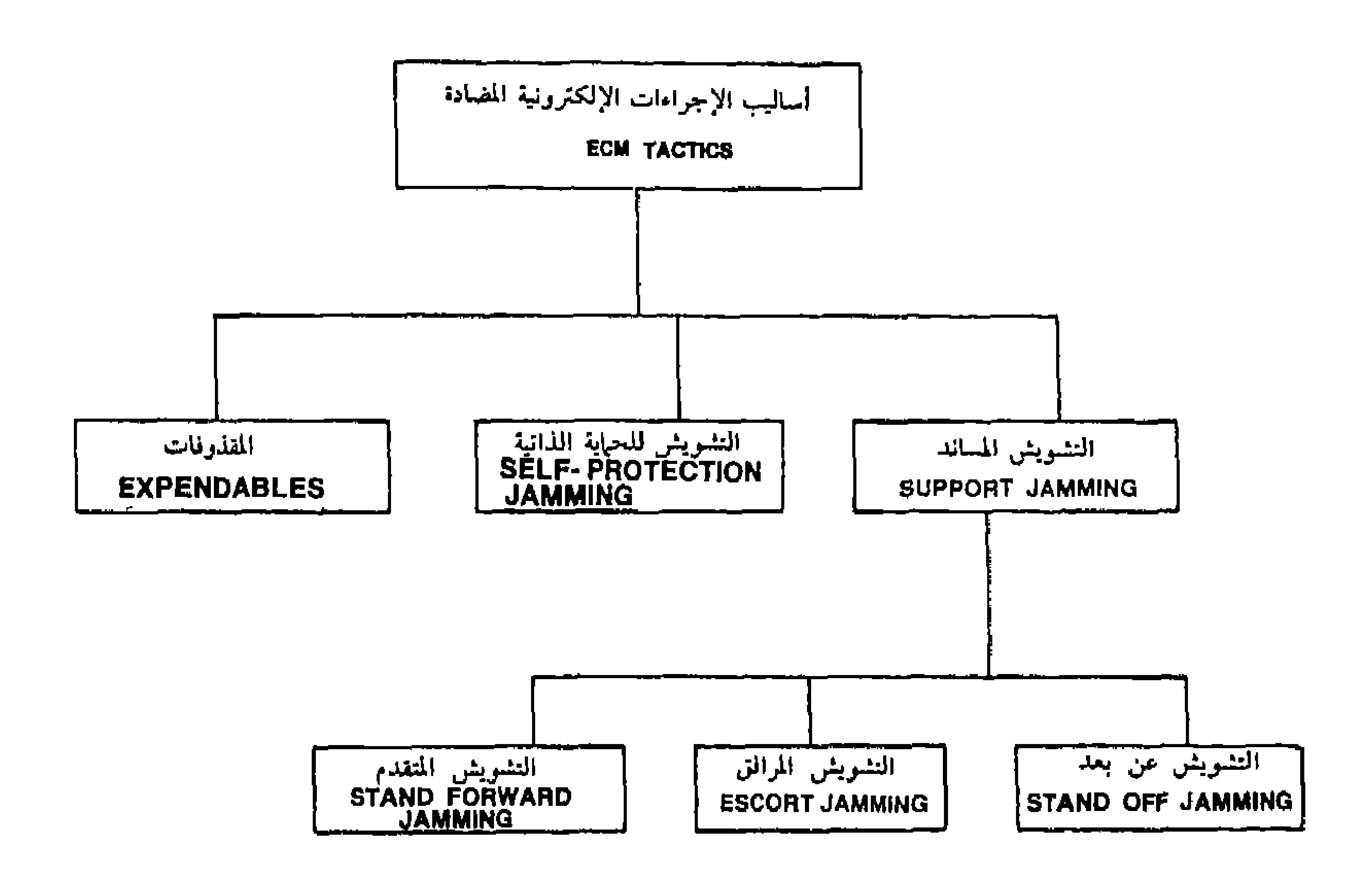
١ ـ تصميم حجم وشكل الطائرات بحيث يعمل هذا على تقليل كمية عكس أشعة رادار العدو.
٢ ـ أن يكون معدن الطائرة ذا قابلية لعكس أقل كمية من أشعة رادار العدو.
٣ ـ أن يكون طلاء الطائرة ذا قابلية شديدة لإحتواء وامتصاص أكبر قدر ممكن من أشعة رادار العدو.

وقد اهتم الأمريكيون بهذه العوامل الثلاثة خاصة في الطائرة القاذفة العملاقة الجديدة (B - 1B)

جـ ـ أساليب الإجراءات الإلكترونية المضادة : ECM TACTICS

سنتطرق هنا إلى بعض أساليب استخدام أجهزة الإجراءات الإلكترونية المضادة، لنتصور معا كيفية التأثير على أجهزة العدو ومعداته بأساليب مختلفة في حالات مختلفة لنحصل على النتيجة المرجوة من التشويش والتأثير على معداته وأجهزته وأنظمته بهدف منع أو تقليل استفادته منها.

والشكل التالي يوضح بعض الأساليب التي تتبع للتأثير على رادارات العدو :



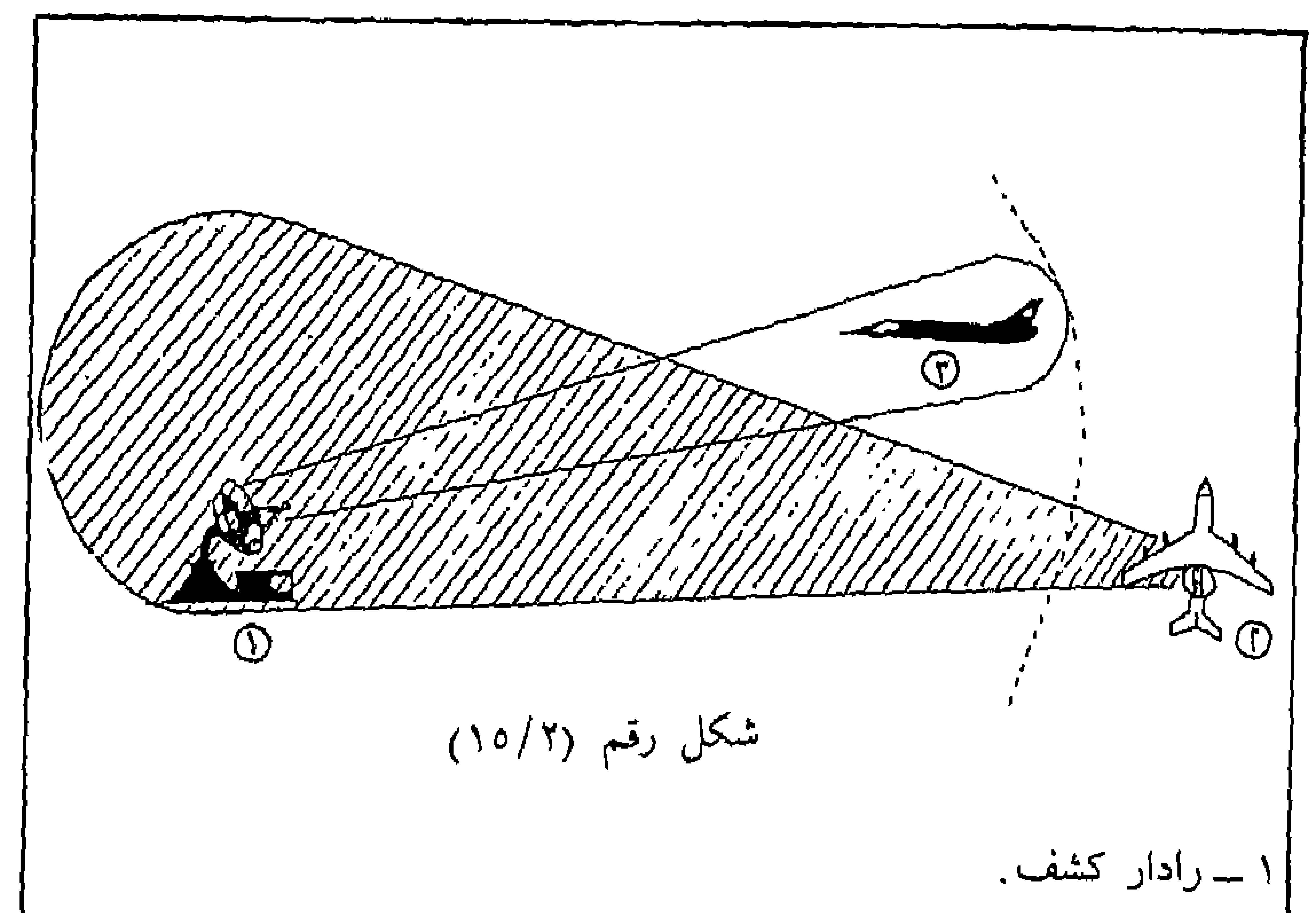
(١) التشويش المساند :

وهو تشويش يستخدم للعمليات الهجومية ويسمى تشويش هجومي (OFFEN- SIVE JAMMING) وعادة يستخدم ضد رادارات الكشف المعادية، وينقسم إلى :

(أ) التشويش عن بعد : STAND-OFF-JAMMING

وهو العملية التي يكون جهاز التشويش الراداري فيها خارج نطاق أو مجال الرادار

المراد التشويش عليه، وكذلك خارج نطاق المعركة أو مسرح العمليات ، ويتطلب هذا أن تكون طاقة التشويش عالية جدا حتى يتم التأثير المطلوب على الرادار المراد التشويش عليه. انظر شكل رقم (٢/١٥).



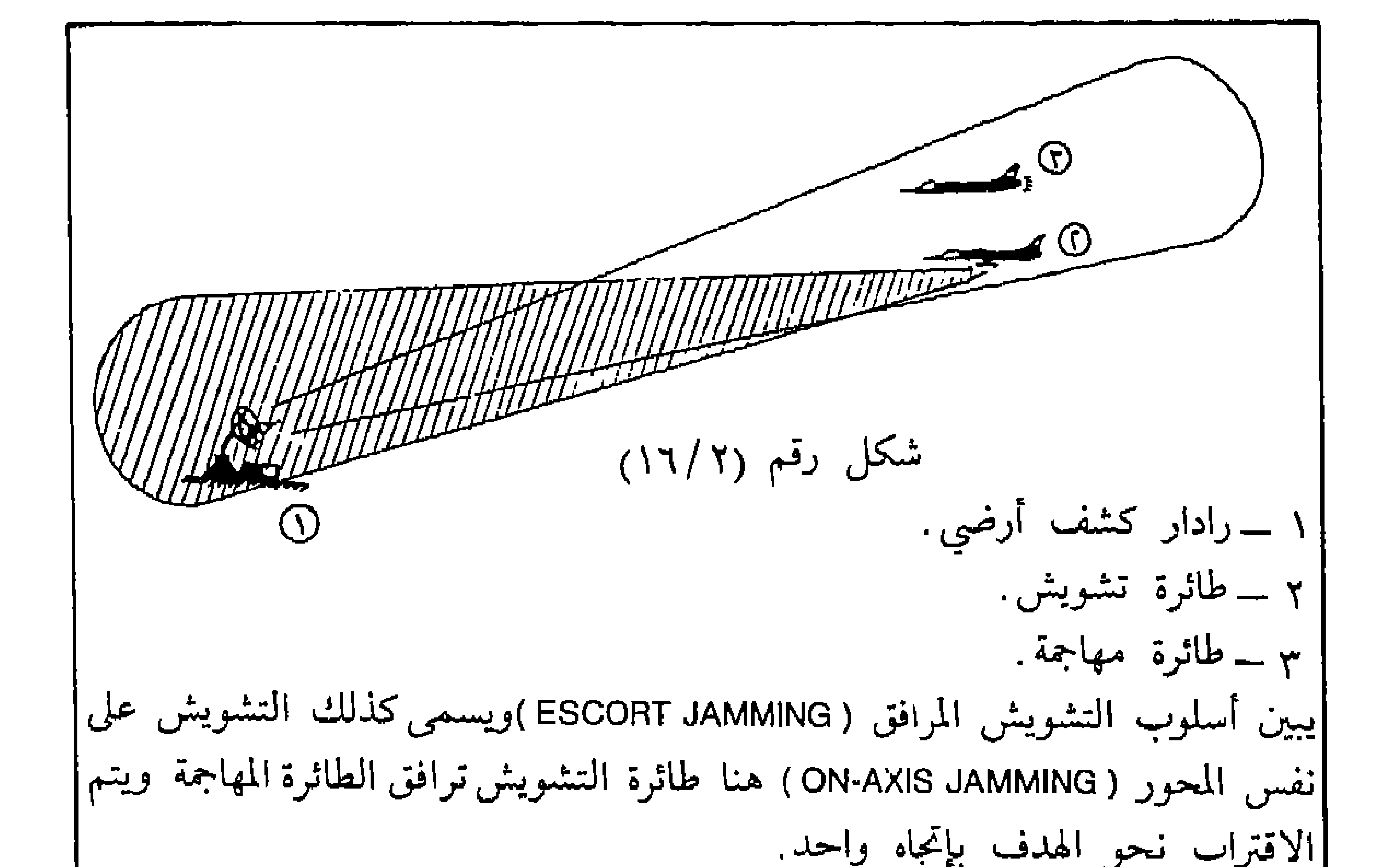
شكل رقم (٢/١٥)

١ ــ رادار كشف.
٢ ــ طائرة تشويش.
٣ ــ طائرة مهاجمة.

يبين الشكل طريقة التشويش عن بعد (STAND OFF JAMMING) عندما تقوم طائرة التشويش (٢) بالتشويش على الرادار الكشفي تقوم الطائرةالمهاجمة بتنفيذ مهمتها.

(ب) التشويش المرافق : ESCORT JAMMING

وهو أسلوب يتبع بوضع جهاز التشويش على طائرة أو سفينة أو آلية مرافقة لسرب من الطائرات لهجوم أو لعملية ما وفي نفس إتجاه الرادار المعادي حتى يفقد العدو القدرة على تحديد مدى وبعد الأهداف (السرب) انظر شكل رقم (٢/١٦). وبالتالي يكون في مقدور الجهاز حماية السرب بكامله من كشف العدو له، أو توجيه أنظمة أسلحته وصواريخه نحوه.



شكل رقم (٢/١٦)

١ ــ رادار كشف أرضي.

٢ ــ طائرة تشويش.

٣ ــ طائرة مهاجمة.

يبين أسلوب التشويش المرافق (ESCORT JAMMING)ويسمى كذلك التشويش على نفس المحور (ON-AXIS JAMMING) هنا طائرة التشويش ترافق الطائرة المهاجمة ويتم الاقتراب نحو الهدف بإتجاه واحد.

(جـ) التشويش المتقدم STAND FORWARD JAMMING

وهو أسلوب يتبع بوضع جهاز التشويش على طائرة وهي تتقدم سرب من الطائرات وتكون الطائرة التي تحمل جهاز التشويش أقرب إلى أجهزة كشف العدو من السرب، وحالما يتم الكشف يقوم الجهاز بالتشويش على أسلحة ومعدات الكشف المعادية حتى يحمي السرب من الكشف، وعادة يستخدم في أسلوب التشويش هذا التشويش المعاد (REPEATER JAMMER) .

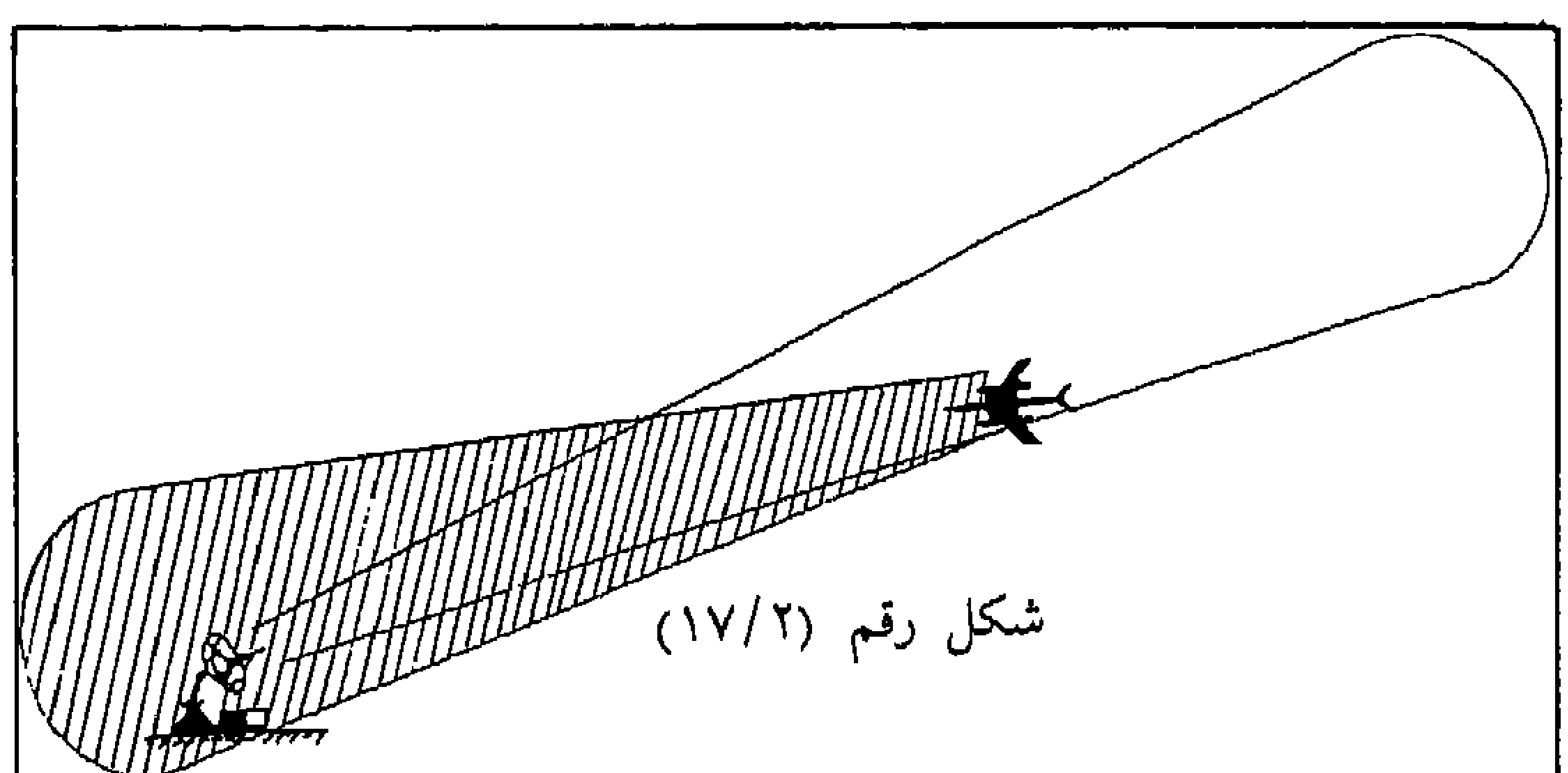
(٢) التشويش للحماية الذاتية : SELF PROTECTION JAMMING (S.P.J.)

وهو أسلوب يتبع بوضع أجهزة التشويش على الطائرات أو السفن أو الآليات المهاجمة لتحمي نفسها من أن تكشفها معدات العدو، أو توجه إليها أنظمة أسلحته وصواريخه وخاصة عندما يستخدم نظام (LOCK-ON) .

وذلك بتسليط أشعة الرادار على الهدف (الذي يحمل هذا النوع من أجهزة التشويش) فحالما يستقبل جهاز التشويش المحمول أشعة رادار العدو يعمل على تحليلها

الكترونيا ليعرف خواص ذلك الرادار ثم يقوم بالتشويش عليه لتعميته وليقلل من فعاليته، واستفادة العدو منه.

وتستخدم هذه النوعية من أجهزة التشويش خاصة عند اختراقه مجال العدو أو عند التوغل داخل أراضيه. انظر شكل رقم (١٧/٢).



يبين عملية التشويش للحماية الذاتية (SELF PROTECTION JAMMING « S.P.J. ») وهو أن تكون نفس الطائرة التي تهاجم موقع العدو، أيضا تحمل أجهزة تشويش لتؤثر وتعيق عمل معدات العدو من رادارات كشف (كما هو مبين بالصورة) أو صواريخ موجهة... الخ حتى تتم الطائرة مهمتها بسلام.

وفي التشويش للحماية الذاتية تستخدم، إما الإجراءات الإلكترونية المضادة الإيجابية (كالتشويش المعاد REPEATER JAMMING) أو الإجراءات الإلكترونية المضادة السلبية (كالنصلات CHAFF) أو كليهما معاً.

٣ ـ المقذوفات : EXPENDABLES OR DESPENCERS

وهو أسلوب تستخدم فيه قاذفات لأجهزة ومعدات التشويش ضد أجهزة ومعدات العدو الكاشفة والحساسة مثل الرادار، بهدف تضليلها ومخادعتها أو التشويش عليها، للتقليل من فعاليتها أو استفادة العدو منها.

وعادة تكون هذه المقذوفات على شكل (CARTRDGES) .

ومن أنواع المقذوفات :

أ ـ النصلات CHAFF

انظر الإجراءات الإلكترونية المضادة السلبية .

ب ـ الطعم : DECOYS

انظر الإجراءات الإلكترونية المضادة السلبية .

جـ ـ الحمم النارية INFRA RED FLARES

وهي عبارة عن حمم أو كرات حديدية ملتهبة تقذف من الطائرات لتضليل ومخادعة الصواريخ (IRGM-INFRA RED GUIDED MISSILE) المضادة للطائرات التي تعمل على تتبع الموجات تحت الحمراء المنبعثة من مؤخرة الطائرة ، أو تقذف من السفن الحربية على شكل قنابل متوهجة لتبعث أشعة تحت الحمراء ، للتشويش وخداع الصواريخ الموجهة نحو الأجسام التي تنبعث منها أشعة تحت الحمراء ويجب هنا التدقيق في هذه العملية إذ تنقسم الصواريخ الموجهة ضد الطائرات والتي تتبع مؤخرة الطائرة إلى قسمين :

أ ـ صواريخ تتبع أعلى درجة حرارة تنبعث من الطائرة وهي عادة تكون داخل محرك الطائرة ، لذلك تراها تلحق الطائرة فقط من الخلف لتنفذ إلى المحرك وتنفجر هناك .

ولأن هذه الصواريخ تتبع أعلى درجة حرارة ، فلو حدث وواجهت الشمس فإنها تنطلق بإتجاهها مخلفة الطائرة المعادية وتلك الصواريخ طراز قديم .

ب ـ صواريخ تتبع موجات معينة من الحرارة وهي الصواريخ الحديثة ، إذ للحرارة موجات تختلف باختلاف درجاتها ، وهذه الصواريخ تتبع موجات معينة من حرارة المحرك . فهي مثلاً تتبع حرارة الـ (ENGINE FLUX) وهي الحرارة الصادرة عن المحرك وتكون على مسافة من ٥ إلى ١٠ أمتار خارج فوهة مؤخرة المحرك ، وهذه تكون درجتها أقل من درجة الحرارة داخل المحرك ، ومن هنا نلاحظ أن هذه الصواريخ لا تتبع فقط مسار مؤخرة الطائرة بل تتبع تدفق حرارة المحرك (FLUX)

وبذلك فلهذه الصواريخ درجة إكتشاف وتتبع أوسع من الصواريخ السابقة.

وقد استخدم الإسرائيليون هذه الحمم النارية بصورة كبيرة في حرب ١٩٧٣ ضد سام ٧ «سترلا» وفي معظم غاراتهم على لبنان.

كما أن هناك أجهزة توضع عادة في مؤخرة الطائرة لتحذر من اقتراب الصواريخ الموجهة بالأشعة تحت الحمراء (IRGM-INFRA RED GUIDED MISSILE) والتي تتجه نحو محرك الطائرات، ويطلق على هذه الأجهزة اسم : (IRWR-INFRA RED WARNING RECEIVER) وحتى الطائرات التجارية بدأت بالتفكير في استخدام هذه الأجهزة لتنذرها من تلك الصواريخ وخاصة سام ٧ الروسية الموجودة لدى بعض الإرهابيين (وتفيد المصادر أن حوالي ٢٥٠ ألف صاروخ سام ٧ موجودة في العالم لا يعرف مالكوها)، وتحمل أيضا أجهزة تشويش ضد ذلك النوع من الصواريخ يسمى (IRCM-INFRA RED COUNTER MEASURERS)
وهي أجهزة تشويش مضادة لتلك الصواريخ.

ولعل هذا يفيد في تجنب ما حدث في بلدة روديسيا الإفريقية عندما هاجم بعض الإرهابيين طائرة نقل تجارية مستخدمين صواريخ سام ٧.

د ــ أجهزة التشويش المقذوفة :

EXPENDABLES OR DISPENSERS JAMMERS

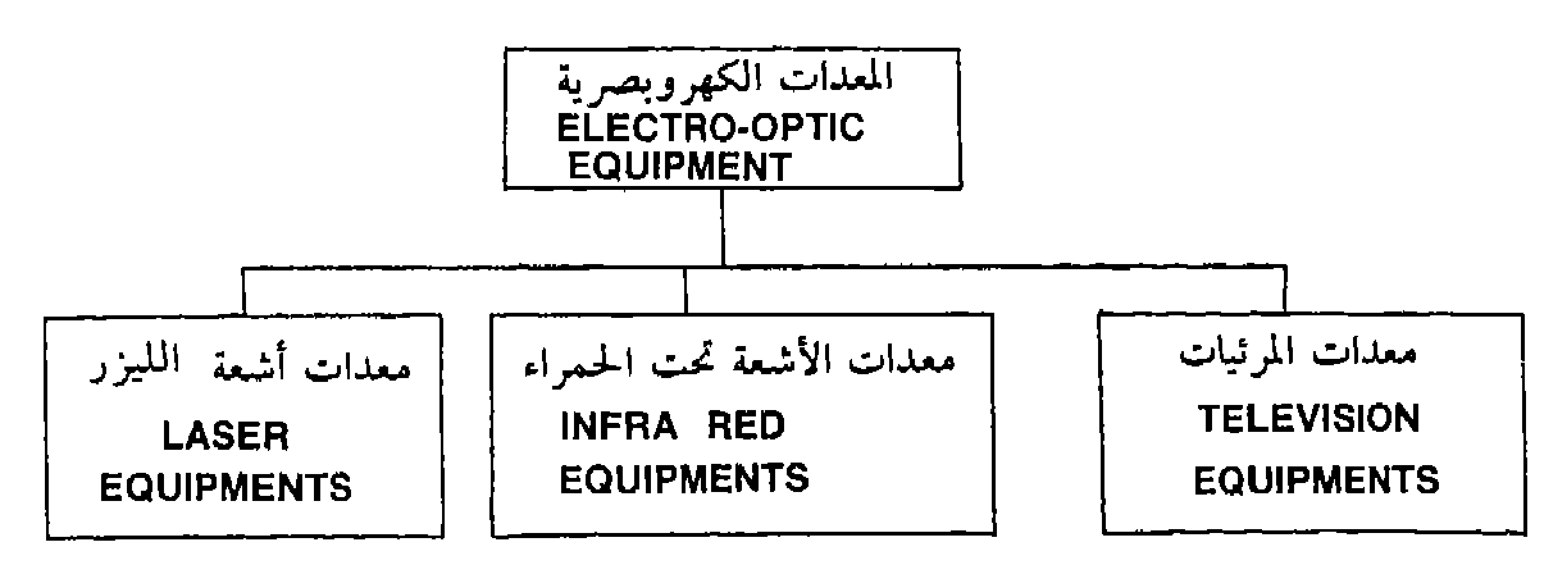
وهي أجهزة تقذف من آليات أرضية أو طائرات أو سفن حربية، قرب مواقع العدو لكي تشوش على راداراته أو اتصالاته لمدة معينة حسب طاقة بطارية الجهاز المشوش وهذه الأجهزة عادة إما أن تسقط إسقاطا من الطائرات أو تقذف بقذيفة تهبط بعدها بمظلة (باراشوت) وفي الغالب تكون أجهزة مموهة، أي يكون شكلها ولونها مناسبا للبيئة التي توضع فيها حتى يصعب على العدو رؤيتها وابطال مفعولها.

د ــ الإجراءات المضادة الكهروبصرية : ELECTRO-OPTIC COUNTER MEASURES (E.O.CM)

المعدات الكهروبصرية : ELECTRO-OPTIC EQUIPMENTS

المعدات الكهروبصرية أو الكهروضوئية هي المعدات التي لها علاقة بالذبذبات أو بالترددات التي تستجيب لها عين الإنسان فتبصر الأشياء التي انعكست عنها أو انبعثت منها تلك الذبذبات، أو بالذبذبات المقاربة للذبذبات التي تستجيب لها عين الإنسان فتظهرها تلك المعدات وتحولها إلى ذبذبات تستجيب لها عين الإنسان.

وتنقسم تلك المعدات إلى :



ــ معدات المرئيات : TELEVISION EQUIPMENTS

وهي المعدات التي يستعين بها الإنسان لرؤية أو لتصوير الأشياء التي يستطيع رؤيتها بعينة المجردة، وهي تستخدم عادة لإظهار الأشياء (الأهداف) على هيئة صورة أو فيلم.. الخ، لتكبير حجم الأهداف في الصورة لرؤيتها بوضوح أو لتقريب صورة الأهداف إذا كانت بعيدة أو لتمييز الأهداف عن قرب أو للكشف عن الأهداف. ومن هذه المعدات أجهزة تلتقط أضواء النجوم والقمر وأضواء المصادر الأخرى المنعكسة عن الأهداف فيستطيع الإنسان رؤية تلك الأهداف في الليل بوضوح.

ــ معدات الأشعة تحت الحمراء INFRA RED EQUIPMENTS

وهي المعدات التي يستعين بها الإنسان لرؤية أو لتصوير الأهداف التي لا يستطيع رؤيتها بعينة المجردة وخاصة في الظلام لأن تنبعث منها أو تنعكس عنها ذبذبات أعلى من الذبذبات التي تستجيب لها عين الإنسان، وخاصة الأشياء التي تشع حرارة أكثر من صفر كالفن كالإنسان أو (السيارة أو الطائرة الحديثة التشغيل.. الخ).

ـ معدات أشعة الليزر : LASER EQUIPMENTS (أنظر صفحة ١٠٤) .

* ـ الإجراءات المضادة الكهروبصرية : ELECTRO-OPTIC COUNTER MEASURES (EOCM)

هي « العمليات التي تستخدم فيها أساليب ومعدات مختلفة للتأثير على معدات العدو الإلكترونية (الكهروبصرية) الفعالة لمنع أو تقليل أستفادته منها ». هناك معدات وأجهزة إلكترونية تستخدم للكشف والاستطلاع، تعتمد على استقبال موجات كهرومغناطيسية ـ وبالذات موجات كهروبصرية أي الموجات التي يستطيع الإنسان استقبالها بعينة المجردة وهي تتراوح بين (٤٢٠×١٠^١٢ هرتز و٧٥٠×١٠^١٢ هرتز وهي الموجات أو الذبذبات الضوئية (بصرية) (LIGHT FREQUENCIES) .

فعندما تستقبل عين الإنسان هذه الموجات على هيئة حزم ضوئية، تتكون لديه صورة، هي صورة الأشياء التي أمامه، والإنسان يرى فقط الأجسام أو الأشياء التي تنبعث منها موجات ضوئية كالشمس أو الأجسام التي تعكس الموجات الضوئية كالقمر، وهذه هي نفس عملية الكاميرات العادية والتلفزيونية فهي تستقبل الموجات الضوئية وتظهرها على هيئة صور وأفلام .

وبنفس الأسلوب هناك بعض أنظمة الأسلحة التي تستعمل الموجات الضوئية للكشف والتوجيه مثل الصاروخ الموجه تلفزيونيا (T.V. GUIDED MISSILE) فهنا يقوم مشغل الصاروخ الموجه تلفزيونيا بمراقبة الأهداف التي تنبعث أو تنعكس منها موجات ضوئية (بصرية) بشاشة تلفزيونية ثم يركز على هدف معين ويطلق الصاروخ نحوه .

ونلاحظ هنا أن معدات الكشف هذه المعتمدة على الموجات الضوئية المنبعثة أو المنعكسة من الأهداف المراد كشفها هي معدات سلبية أي أنها فقط تستقبل الموجات الضوئية المنبعثة أو المنعكسة من الأجسام فتكتشفها، لكن هناك معدات كاشفة تعتمد على الموجات الضوئية ولكنها معدات ايجابية إذ ترسل ضوءا نحـو الأهداف وتستقبله فتكتشفها وتركز عليها ثم توجه الأسلحة نحوها وهذه هي فكرة استخدام أشعة الليزر عسكريا (كالصاروخ الموجه بأشعة الليزر (LASER GUIDED MISSILE) لكن هناك بعض الأجهزة الكشفية السلبية المعتمدة على الأشعة تحت الحمراء وتسمى (IR SENSORS) والأسلحة الموجهة نحو الأهداف التي تتبع الموجات تحت الحمراء المنبعثة من الأهداف (كالصاروخ الموجة بالأشعة تحت الحمراء (IR GUIDED MISSILE) .

لكن بعض المراجع والأنظمة تفصل مجالات الأشعة تحت الحمراء عن الإجراءات المضادة الكهروبصرية (EOCM) فالإجراءات المضادة الكهروبصرية (EOCM) هي العمليات التي تستخدم فيها أساليب ومعدات مختلفة للتأثير على المعدات الكشفية المعادية التي تعتمد على الموجات البصرية (الضوئية).

ولقد استخدمت بعض الأساليب والمعدات منذ القدم كإجراءات مضادة لعين الإنسان مثل: استخدام الدخان لحجب الرؤية، وإثارة الغبار أمام العين، واستغلال وقت الضباب المنخفض، وإجراء بعض التمويهات (CAMOUFLAGE) على المعدات والمواقع لخداع نظر العدو.

ولقد استخدمت هذه الطرق في الحروب بصورة أكثر فنية وتقنية ومن أمثلة ذلك :

في الحرب العالمية الثانية استخدم الألمان فكرة خداع النظر عندما أراد الإنجليز قصف منطقة صناعية عسكرية في مدينة هامبورغ الألمانية وكانت المنطقة تقع بالقرب من جسر وجزيرة في النهر، فموه الألمانيون الجسر والجزيرة بإقامة جزيرة وجسر مصطنعين، فقصف الإنجليز مكانا بعيدا نسبيا عن المنطقة الصناعية العسكرية المقصودة.

وفي حرب ١٩٧٣ استطاعت إحدى الدول العربية المواجهة وضع بطاريات سام ٢ و٣ من البلاستيك في أماكن متفرقة من الجبهة، وقد نجحت هذه الفكرة إذ تجنب الإسرائيليون تنفيذ عملياتهم في تلك المناطق.

والآن سنأخذ استخدامات أشعة الليزر كمثال للإجراءات الكشفية والإجراءات المضادة للموجات الكهروبصرية (EOCM).

أشعة الليزر :

LASER-LIGHT AMPLIFICATION BY STIMULATED EMISSION OF RADIATION

وهي تعني: تكبير الضوء بطريقة الإنبعاث المتحدد للإشعاع.

هي عبارة عن موجات ضوئية كهرومغناطيسية ذات طيف ضيق من الترددات، (أو تردد واحد فقط)، وتستعمل أشعة الليزر من الناحية العسكرية في عدة أمور، أهمها :

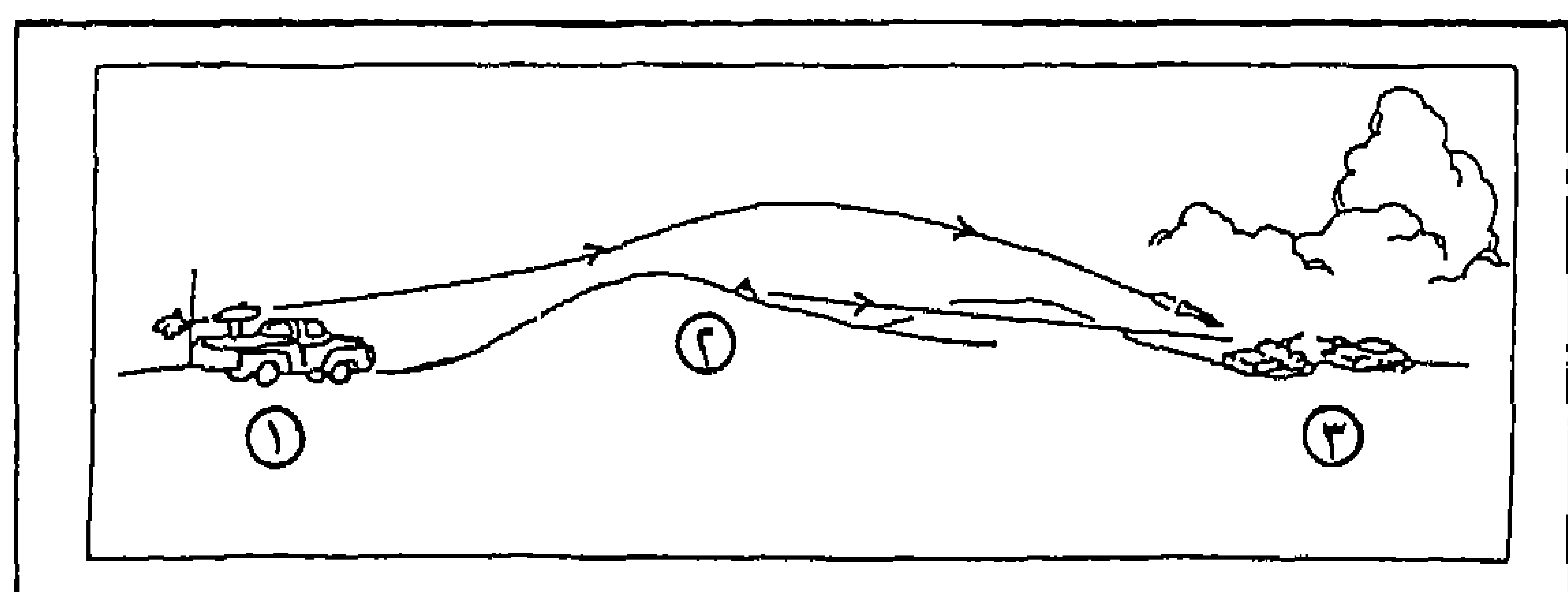
(أ) ــ أشعة ليزر لتقدير المسافات :

وجهاز أشعة الليزر في هذه الحالة يطلق نبضات شعاعية باتجاه الهدف ثم تعود فتستقبل الأشعة المنعكسة عنه، تماما كما هي الحال بالنسبة للرادار فالتشويش هنا يحدث بقيام الهدف ببث أشعة ليزر أخرى قد تفيد في خداعه عند تقدير المسافات.

(ب) ــ أشعة الليزر لتوجيه الصواريخ :

وجهاز أشعة الليزر لتوجيه الصواريخ يعرف باسم (LASER DISGNATOR) وهو يسلط أشعة الليزر نحو الهدف بالضبط وبالتحديد في مكان معين منه ثم ينطلق الصاروخ نحو الهدف بخط مستقيم تابعا أشعة الليزر الموصلة إلى الهدف. انظر شكل رقم (٢/١٨).

والتشويش هنا يتم بقيام الهدف نفسه بإطلاق شعاع أكثر شدة بإتجاه هدف كاذب بحيث يجعل الصاروخ يتجه نحو مسار الشعاع المنعكس عن الهدف الكاذب لأنه أكثر شدة وإغراء من شعاع الجهاز الحقيقي الموجه للصاروخ، أو بإطلاق سحابة دخان كثيف .



شكل رقم (٢/١٨)

يبين كيفية استخدام الصاروخ الموجه بأشعة الليزر (LAZER GUIDED MISSILE) لتدمير مواقع العدو التي في ما وراء حاجز أو الأفق.

١ ــ محطة انطلاق الصاروخ.

٢ ــ جهاز يسلط أشعة الليزر نحو الهدف ليتبع الصاروخ تلك الأشعة ويصيب الهدف (LASER DESIGNATOR).

٣ ــ موقع العدو المراد تدميره.

(جـ) ـ أشعة ليزر لتدمير أسلحة العدو وأجهزته :

ويستعمل هنا جهاز ليزر يطلق شعاعا ذا تركيز عال وقدرة كبيرة من شأنه إذا سلط على معدات العدو أن يعطلها أو يحرقها ويسمى شعاع الموت (DEATH RAY) وهو أكثر استعمالا فيما يسمى بحرب النجوم وأيضا تستخدم « أسلحة الجزئيات الإشعاعية » التي تطلق جزئيات نووية ضخمة يمكن نشرها في الفضاء حيث تقوم بإسقاط الأقمار الصناعية والصواريخ .

وقد قام سلاح الطيران الأمريكي بتجربة ناجحة في نهاية شهر يوليو ١٩٨٣ بمنطقة التجارب بولاية كاليفورنيا تمثلت في تدمير صواريخ «سايدويندر» وهي صواريخ جو ـ جو باستخدام أشعة ليزر، حيث أطلقت طائرة أمريكية مقاتلة خمسة من هذه الصواريخ التي تطير بسرعة ٣٢٠٠ كم / ساعة وقبل أن تصل هذه الصواريخ إلى أهدافها أطلقت عليها طائرة أخرى أحزمة من شعاع ليزر فدمرتها. وقد كشف النقاب عن هذا النوع من السلاح الرئيس الأمريكي رونالد ريغان في مقابلة تلفزيونية.

والجدير بالذكر أنه قد سبق هذه التجربة تجربة أخرى فاشلة أجراها الأمريكيون لنفس الغرض (تدمير صواريخ جو ـ جو بأشعة الليزر) في ١٩٨١/٧/٢م[1].

د ــ كذلك تستخدم أشعة الليزر في مجال الإتصالات والأقمار الصناعية.

التشويش على أشعة الليزر المدمرة :

١ ــ ذكرت المصادر أن السوفيات استطاعوا تشتيت أشعة الليزر المدمرة بقذف شحنات من الرمال بإتجاه أشعة الليزر.

٢ ــ العمل على تغليف المعدات المراد تدميرها بأشعة ليزر بغلاف من مادة ذات قدرة عالية على عكس تلك الأشعة وشتيتها، لكن من مساوىء هذه الطريقة أنها تجعل من المعدات هدفا واضحا أمام رادارات العدو[2] .

٣ ــ العمل على تغليف موقع المعدات المراد تدميرها بأشعة الليزر بدخان يصعب على أشعة الليزر النفاذ منه[3] .

(١) مجلة INTERNATIONAL DEFENCE REVIEW عدد ١٩٨١/٦م. ص ٧٠٥.
(٢) انظر كتاب الحرب الإلكترونية لكمال السعدي طبعة ١٩٧٩ صفحة ١٤٢.
(٣) أنظر المصدر السابق .

هـ ـ التشويش النووي أو النبضة الكهرومغناطيسية النووية :

NUCLEAR ELECTROMAGNETIC PULSE (NEMP)

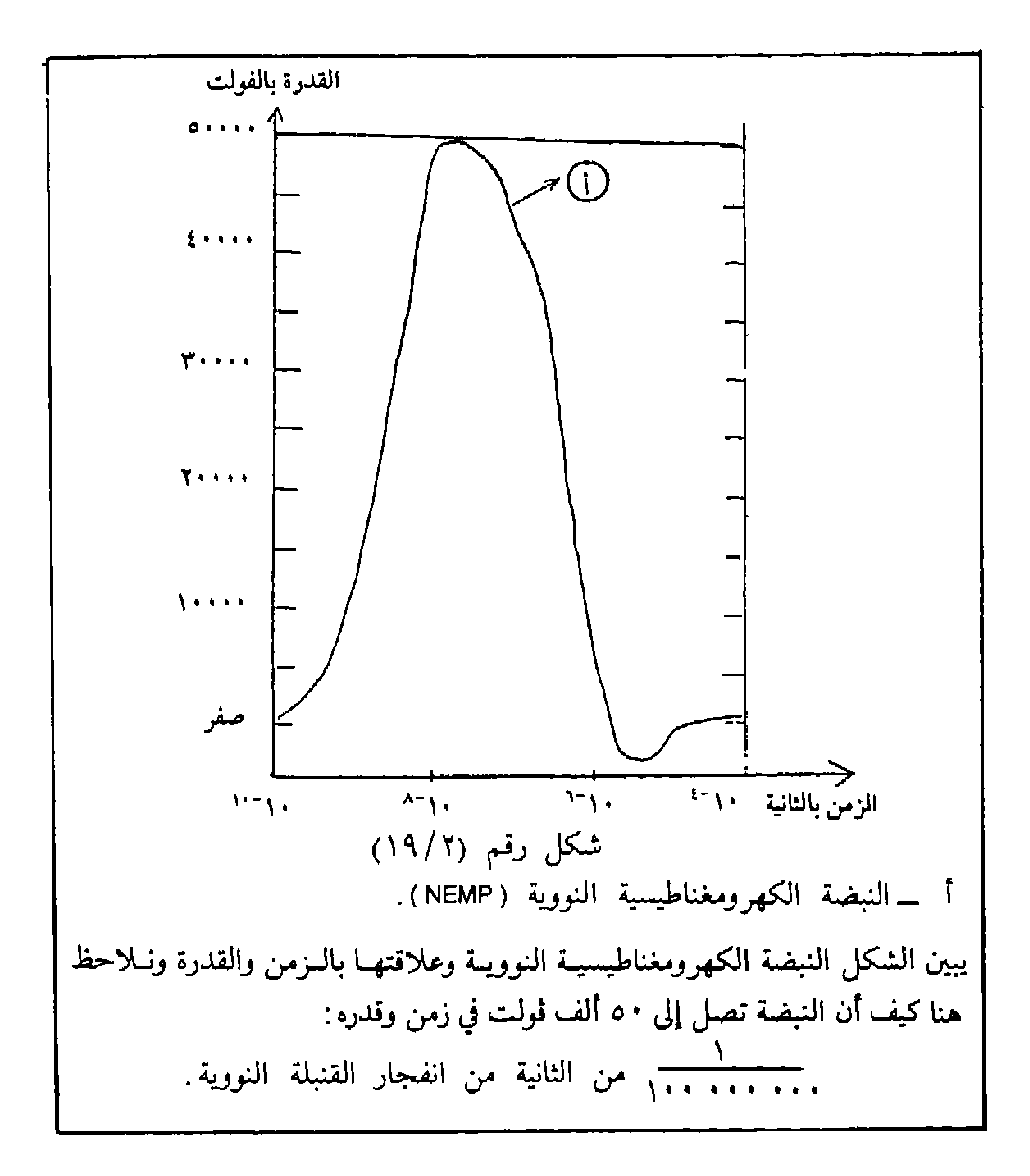
والآن وبعد أن انتهينا من شرح الأساس الثالث « الإجراءات الإلكترونية المضادة » يجب أن لا نغفل نوعا مميزا من أنواع التأثيرات على الأجهزة الإلكترونية بجميع أشكالها وأنواعها واستخداماتها، إذ أن هناك نوع آخر من التشويش أو التأثير أو التعطيل على الأجهزة الإلكترونية، ويطلق عليه التشويش النووي أو النبضة الكهرومغناطيسية النووية : (NUCLEAR ELECTROMAGNETIC PULSE (NEMP))

وهو عبارة عن نبضة (PULSE) قوية جدا تصل قدرتها إلى عشرات الآلاف من الوات تحدث في غضون جزء من المليار من الثانية مباشرة بعد انفجارقنبلة نووية[1]، كما تستغرق جزءا من المليون من الثانية وبعدها تنتهي. انظر شكل رقم (٢/ ١٩) وصفات هذه النبضة تجعلها تعطل وتشل جميع الأجهزة الإلكترونية والكهربائية الموجودة في مجال القنبلة النووية وأيضا خارج ذلك المجال انظر شكل رقم (٢/ ٢٠) إذ أن لها تدميراً يتناسب مع قرب الأجهزة وبعدها عن موقع التفجير، كما يعتقد أن تلك النبضة قد تؤثر تأثيرا خطيرا على الإنسان، وتحدث هذه النبضة إما على سطح الأرض إذا كانت القنبلة النووية منفجرة على سطح الأرض، أو في طبقات الجو العليا عندما تنفجر القنبلة النووية هناك معطلة الأجهزة الموجودة في الأقمار الصناعية والطائرات، ثم تتجه النبضة إلى الأرض بفعل المجال المغناطيسي الأرضي (EARTH MAGNATIC FILED) معطلة كذلك الأجهزة الأرضية. ويقال أنه إذا انفجرت قنبلة نووية على ارتفاع شاهق فوق وسط الولايات المتحدة فإن قوة النبضة سوف تؤثر على جميع الأجهزة والمعدات في الولايات المتحدة الأمريكية بأكملها.

ويطلق على هذا التشويش أو التعطيل لجميع أنواع الأجهزة والكيبلات. . الخ. بفعل تلك النبضة اسم (POTENTIAL CRIPPLER).

---

(١) مجلة COMMUNICATIONS INTERNATIONAL عدد أكتوبر ١٩٨٤م صفحة ٦٩.



شكل رقم (١٩/٢)

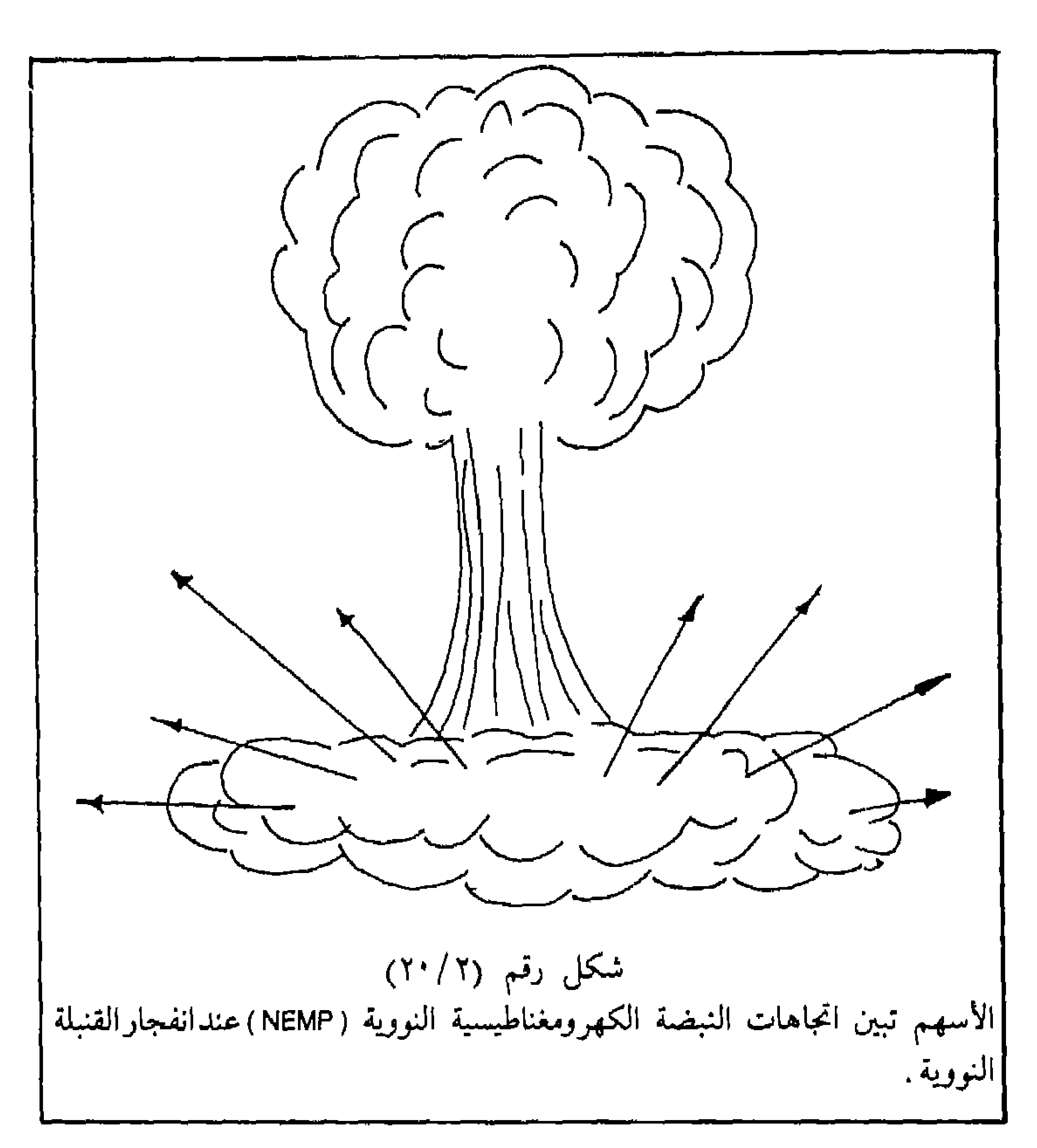
أ ـ النبضة الكهرومغناطيسية النووية (NEMP).

يبين الشكل النبضة الكهرومغناطيسية النووية وعلاقتها بالزمن والقدرة ونلاحظ هنا كيف أن النبضة تصل إلى ٥٠ ألف ڤولت في زمن وقدره:

$\frac{١}{١٠٠ ٠٠٠ ٠٠٠}$ من الثانية من انفجار القنبلة النووية.

عرف هذا النوع من التشويش أو التعطيل للأجهزة في أوائل الستينات، عندما كان السوفييت والأمريكيون يقومون بتفجير قنابلهم النووية التجريبية في المحيط الهادى، إذ لوحظ أن جميع خطوط الهاتف في جزر هاواي قد عطلت تماما وكانت تلك الجزر قريبة من مكان التفجيرات.

ومنذ ذلك الوقت أدرك السوفييت والأمريكيون أن هذا النوع من التشويش أو



شكل رقم (٢/٢٠)
الأسهم تبين اتجاهات النبضة الكهرومغناطيسية النووية (NEMP) عندانفجار القنبلة النووية.

التعطيل له مشكلة كبيرة وحلها صعب جدا وقد كان الحل الوحيد الشائع آنذاك هو البعد عن مكان التفجير للوقاية من ذلك التشويش والتعطيل.

وقد تزايد الإهتمام بهذا الموضوع في الدول الغربية خاصة في عام ١٩٨٢م عندما أثيرت ضجة حول كيفية الوقاية من هذا النوع من التشويش والتعطيل.

والنبضة الكهرومغناطيسية النووية لها قابلية الإمتصاص من قبل معظم المعادن كما أنها تسري في المعادن والكيبلات وفوق الإشارات الكهربائية والإلكترونية (CARRIED BY SIGNALS) لتقوم بتعطيل الأجهزة واحدا تلو الآخر وهي في طريقها المتنقل، وكلما

كانت المعادن والأجهزة كبيرة الحجم إمتصت أكبر قدر من طاقة النبضة فيكون التأثير أو التشويش أو التعطيل أكبر، وكذلك الهوائي العريض المجال BROAD BAND) (ANTENNA يمتص أكبر قدر من النبضة أكثر من الهوائي الضيق المجال NARROW) (BAND ANTENNA وهكذا . . .

فعندما تدخل هذه النبضة عن طريق الهوائيات أو الكيبلات مثلاً، وتسري في الأجهزة الإلكترونية الحساسة مثل الترانزستور والصمامات والفيوزات بطاقتها وجهدها العالي جداً تحرقها وتدمرها بسرعة هائلة فيتعطل الجهاز. تماما كما يحدث عن تشغيل جهاز كهربائي - كالراديو أو المكيف - وفجأة يحترق الفيوز (FUSE) وذلك بسبب وجود جهد كهربائي عالي جداً أكبر من أن يتحمله الفيوز فيحترق فيتعطل الراديو أو المكيف .

وهذه النبضة لها تأثير كبير جداً على MODERN MICRO SEMI CONDUCTORS) (ELFCTRONICS الموجودة في معظم الأجهزة المتطورة والحديثة على اختلاف أنواعها وإستعمالاتها المدنية والعسكرية مثل أجهزة الكمبيوتر والراديو والرادارات والأقمار الصناعية والطائرات وأجهزة السفن والأجهزة الملاحية والتليفونات والتلفزيونات ومحطات الكهرباء وأجهزة السكك الحديدية والأجهزة الطبية وأجهزة المصانع . . . الخ .

وقد لوحظ أن هذه النبضة (القاتلة) لها تأثير قليل على الأجهزة القديمة خاصة التي تستعمل الصمامات القديمة .

وقد استنتج الخبراء الأمريكيون ذلك عندما فككوا الأجهزة الإلكترونية الموجودة في طائرة ميج ٢٥ وحللوها، وذلك عندما هرب بها طيار سوفياتي إلى اليابان عام ١٩٧٥ . وقد تعجبوا لوجود تلك الصمامات القديمة في هذه الطائرة الحديثة المتطورة ولكن بعد الدراسة المستفيضة استنتجوا أن السبب يعود إلى رغبة السوفييت في تقليل تأثير النبضة الكهرومغناطيسية النووية على أجهزة الطائرة.

ولقد حاول السوفييت إنتاج أجهزة لتوليد هذا النوع من النبضات بدلاً من الحصول عليها من انفجار القنبلة النووية وذلك لكي توضع في طبقات الجو العليا موجهة نحو الأرض لتعطيل الأجهزة السفلى وخاصة الصواريخ الأمركية العابرة للقارات .

وهذا النوع من النبضات قد يحدث أيضا من الصواعق أو الأجهزة كما ذكرنا والاختلاف الرئيسي بينهما هو حدة وقوة طاقة النبضة.

وهناك بعض الطرق التي تفيد في التخلص أو التقليل من تأثير التعطيل أو التشويش الناتج عن تلك النبضة منها:

مصيدة النبضة (EMP ARRESTER) وهي دائرة كهربائية توضع في مداخل الأجهزة (EQUIPMENT INPUTS) لتصطاد هذه النبضة أو تقلل من طاقتها بسحبها إلى الأرضية (DRAIN IT TO GROUND) قبل أن تصل قلب الجهاز.

وهذه الدائرة يجب أن تكون سريعة جدا للتجاوب مع النبضة (QUICK RESPONSE) كما يجب أن تتميز بقوة تحمل كبيرة للنبضة ومما يجدر ذكره أن هذا النوع من الدوائر الكهربائية مكلف جدا، بالإضافة إلى أنه غير مضمون النتائج.

وهناك نوع خاص من الدوائر الإلكترونية مصنوعة لكي تقلل من تأثير النبضة النووية يطلق عليها (RADIATION HARDENED CIRCUITS)

و ـ التداخل : INTERFERENCE

هو « أية إشارة غير مرغوب فيها تدخل في الأجهزة والدوائر الكهربائية والإلكترونية ».

وهذا الإشارة (SIGNAL) إما أن تكون إشارة كهرومغناطيسية (ELECTRO-MAGNETIC SIGNAL) تدخل وتقحم نفسها في الجهاز (وخاصة أجهزة الإستقبال) آتية عبر الأثير أو تكون إشارة كهربائية (ELECTRICAL SIGNAL) تدخل في الجهاز آتية عبر الأسلاك الكهربائية والكيبلات.

وهذه الإشارة غير المرغوب فيها تؤثر على الأجهزة الكهربائية والإلكترونية وقد تشوش عليها فتقلل من فعالية الجهاز وقد تعيق الجهاز عن أداء مهمته وقتيا أو دائم التأثير، ويتفاوت هذا التأثير بتفاوت قوة الإشارة المتداخلة.

وعادة يكون هذا التأثير على شكل ضوضاء أو ضجيج (NOISE) أو نبضات، ومن خصائص التداخل صعوبة معرفة مصدره سريعاً .

والتداخل كما نلاحظ كلمة شاملة، تشمل جميع الأسباب التي تؤدي إلى خلل أو تأثير أو تشويش على الأجهزة الكهربائية أو الأجهزة الإلكترونية وخاصة أجهزة الاستقبال، ومن ضمنها أيضا الإجراءات الإلكترونية المضادة. وهناك أنواع كثيرة من مصادر التداخل سنذكر فيما يلي بعضا منها :

(١) التداخل المقصود :

(MANMADE INTERFERENCE) INTENTIONAL INTERFERENCE

وهو التداخل الناتج عن تأثير أجهزة العدو (أجهزة الإجراءات الإلكترونية المضادة) على أجهزتنا وذلك عن عمد وقصد عدائي وبطريقة مباشرة أو غير مباشرة. وهو نوع من أنواع التشويش، ويكون عادة تداخل كهرومغناطيسيا.

(٢) التداخل غير المقصود (التداخل العرضي) ACCEDENTIAL INTERFERENCE

وهو التداخل الناتج عن وجود أجهزة ارسال صديقة ترسل بنفس الذبذبة التي نرسل عليها في نفس الزمن بالصدقة المحضة، وينتج عن ذلك تأثير أو تشويش يؤثر على

أداء أجـهزتنا المستقبلة، وهذا النوع من التداخل يحدث عادة أثناء المعارك والحروب بسبب كثرة الإرسال والإستقبال في منطقة معينة، ويكون عادة تداخلا كهرومغناطيسياً.

(٣) التداخل الطبيعي : NATURAL INTERFERENCE

وهو التداخل الناتج عن وجود عوامل طبيعية مثل البرق والعواصف الترابية والثلجية والإشعاعات الكونية الآتية من الأجرام السماوية الموجودة في الفضاء الخارجي كالشمس وغيرها، وبالإشعاعات اللاسلكية الحرارية التي تنشأ من القشرة الأرضية والغلاف الجوي.

وهناك مثلاً ظاهرة كونية تسمى (MOGEL-DELLINGER) ، هذه الظاهرة تحدث كل سنتين أو أربع سنوات مرة، تؤثر على جميع الترددات من ١ إلى ١٥ ميغا هرتز بحيث لا تسمع أي اتصالات في ذلك المجال، وهي عادة تحدث لمدة ساعة أو ساعتين تقريبا أثناء النهار (عصرا).

كما أن هناك عوامل أخرى قد تندرج تحت هذا النوع من التداخل وهو تداخل ناتج عن أشياء من صنع الإنسان مثل :

محطات الإذاعة، محطات الكهرباء، المحولات الكهربائية، الأسلاك الكهربائية ذات الطاقة العالية، المصانع، أجهزة تشغيل المحركات مثل (CAR IGNITION) ، لذا نرى معظم الأجهزة الحديثة محاطة بنوع من الشبكة أو الحاجز يحمي الكيبل أو الجهاز من هذا النوع من التأثيرات الأخيرة وتسمى هذه العملية بـ (EQUIPMENT SHEILDING) ونراها متمثلة بالـ (CO-AXIAL CABLE) وقد يكون التداخل الطبيعي تداخلا كهربائياً أو كهرومغناطيسيا.

(٤) التداخل الداخلي : INTERNAL INTERFERENCE

وهو التداخل الناتج عن وجود خلل داخل نفس الجهاز الإلكتروني أو الكهربائي ويكون عادة تداخلا كهربائيا من شأنه أن يضعف من أداء عمل الجهاز، وهو من أسهل أنواع التداخل التي يمكن كشفها عن طريق فحص الجهاز.

أو قد يكون تداخلا كهرومغناطيسيا كمثل بعض الدوائر الكهربائية أو الإلكترونية التي تؤثر على الدائرة المذبذبة (OSCILIATOR) فتغير من مقدار التردد. (FREQUENCY).

٤ ـ الأساس الرابع
المضادات الإلكترونية للإجراءات المضادة[1]
ELECTRONIC COUNTER-COUNTER MEASURES (ECCM)

ونذكر بعض التعاريف :

١ ـ التعريف في كتاب : (INTELLEGENCE WARFARE) صفحة ٨١

(ACTIONS TAKEN TO ENSURE FRIENDLY USE OF THE ELECTROMAGNETIC SPECTRUM AGAINST ELECTRONIC WARFARE DESPITE THE ENEMY'S USE OF COUNTER MEASURES).

ومعنى التعريف كالآتي :

الإجراءات المتخذة لضمان استخدام المجال الكهرومغناطيسي الصديق ضد الحرب الإلكترونية رغم استخدام الإجراءات المضادة المعادية.

٢ ـ التعريف في كتاب « الحرب الإلكترونية » لكمال السعدي صفحة ١٠

« وهي مجموعة الخطوات التي يتخذها أحد الأطراف المتحاربة في مواجهة إجراءات الخصم الإلكترونية المضادة لأسلحته ».

وتسمى التدابير المضادة للإجراءات الإلكترونية المضادة.

٣ ـ التعريف في كتاب (ELECTRONIC WARFARE AIRCRAFT) صفحة ١٣

(MEASURES DESIGNED TO NULLIFY OFFENSIVE ACTION AGAINST A FRIENDLY ELECTRO-MAGNETIC SOURCE).

ومعنى التعريف كالآتي :

الإجراءات المصممة لإحباط الإجراء الهجومي المضاد للمصدر الكهرومغناطيسي الصديق.

٤ ـ تعريف شركة هيوز (HUGHES) الأمريكية :

(ACTIONS TAKEN TO MAINTAIN THE USE OF THE ELECTROMAGNETIC SPECTRUM BY FRIENDLY FORCES)

---

(١) وأيضاً تسمى : إجراء ات الحماية الإلكترونية : ELECTRONIC PROTECTIVE MEASURE (E.P.M)

ومعنى التعريف كالآتي :

الإجراءات المتبعة للمحافظة على استخدام المجال الكهرومغناطيسي من قبل القوات الصديقة.

٥ ـ تعريف من شركة راكال البريطانية : (RACAL COMMUNICATIONS LIMITED)
(FOR THE PROTECTIONS OF FRIENDLY COMMUNICATIONS FROM HOSTILE ELECTRONIC WARFARE).

ومعنى التعريف كالآتي :

لحماية الإتصالات الصديقة من الحرب الإلكترونية المعادية.

٦ ـ تعريف آخر :

(INVOLVING ACTIONS TAKEN TO INSURE FRIENDLY EFFECTIVE USE OF THE ELECTRO-MAGNETIC SPECTRUM DESPITE THE ENEMY'S USE OF ELECTRONIC WARFARE)

ومعنى التعريف كالآتي :

متضمنا الإجراءات المتخذة لضمان الإستخدام الفعال للمجال الكهرومغناطيسي الصديق رغم استخدام العدو للحرب الإلكترونية.

أما الآن فسنورد تعريفنا نحن للمضادات الإلكترونية للإجراءات المضادة (ECCM) على النحو التالي :

هي **«العمليات التي تستخدم فيها أساليب ومعدات إلكترونية لحماية موجاتنا الكهرومغناطيسية الفعالة المنبعثة من معداتنا المختلفة من استفادة العدو منها أو التأثير على معداتنا»**.

والمعنى هنا هو إتباع أساليب محددة ومعدات إلكترونية متخصصة لحماية موجاتنا الكهرومغناطيسية الفعالة المنبعثة من معداتنا المختلفة مثل أجهزة الإتصال وأجهزة الرادار والأجهزة الملاحية ونظم الأسلحة المختلفة والطائرات والصواريخ . . . الخ من أن يرصدها العدو ويحللها ويعرف مضمونها ويستفيد منها، فتكون إجراءاتنا هنا مضادة للإجراءات الإلكترونية المساندة للعدو وتسمى :

المضادات الإلكترونية للإجراءات الإلكترونية المساندة (ANTI-ESM) وهي أيضا

تستخدم ضد إستخبارات الإتصالات (COMINT) والإستخبارات الإلكترونية (ELINT).

وكذلك إذا أعددنا أساليب محددة ومعدات إلكترونية متخصصة لتحمي معداتنا المختلفة الأخرى من تأثير العدو عليها بأشكال التشويش المختلفة كما عـرفنا في الأساس الثالث ويطلق على هذا النوع من الحماية « المضادات الإلكترونية للإجراءات الإلكترونية المضادة » (ANTI-ECM) وهي لكي تضاد الإجراءات الإلكترونية المضادة للعدو.

كما يمكن أن تكون الإجراءات المضادة إما باستخدام أجهزة إلكترونية متطورة و بإستخدام أساليب فنية أو كليهما، ويتخلص الأساس الرابع بأن تستخدم جميع الطرق التي تكفل الحماية لأجهـزتنا الإلكترونية من رادارات وإتصالات وصواريخ.. الخ من المراقبـة والتشويش. إذ كما عرفنا، لو أحكمنا هذه الحماية فستكون مراقبة العدو لموجاتنا الكهرومغناطيسية المنبعثة من معداتنا المختلفة صعبة أو غير مفيدة وبالتالي لن يعرف الكثير عن قوتنا وتسليحنا وموقفنا، ولن يستطيع كذلك التأثير أو التشويش على أجهزتنا باستخدام إجراءاته الإلكترونية المضادة ومن هنا تكون جميع خططه وعملياته المعتمدة على المراقبة والتشويش غير مجدية مما سيرفع من كفاءة أجهزتنا وعملياتنا الحربية.

وكما قلنا أن هذه الإجراءات التي تتخذ لحماية أجهزتنا تتكون من استخدام أجهزة إلكترونية متطورة أو استخدام أساليب فنية، ولذا يجب توافر الحكمة والدراسة لكي تكون جميع أجهزتنا الإلكترونية وأساليبنا الفنية مؤدية لهذه الغاية وهي الحماية الإلكترونية.

ويختلف الأساس الرابع بشكل خاص عن الأسس الأخرى إذ يجب على كل شخص يتعامل مع الأجهزة الإلكترونية أن يعرفه معرفة جيدة، بخلاف الأسس الأخرى التي يجب على المتخصصين في الحرب الإلكترونية فقط معرفتها.

وسنستعرض بعض هذه الأجهزة الإلكترونية والأساليب الفنية التي تكفل توفير الحماية الإلكترونية.

كما تسمى المضادات الإلكترونية للإجراءات المضادة (ECCM) بمسمى آخر يطلق عليه إجراءات الحماية الإلكترونية(ELECTRONIC PROTECTIVE MEASURES) ويتكون من :

أ ـ الإجراءات الأمنية الإلكترونية : ELECTRONIC SECUIRTY MEASURES

وهي عمليات وإجراءات تقليل أو منع العدو من رصد ومراقبة والإستفادة من معلوماتنا الموجودة في موجاتنا الكهرومغناطيسية المنبعثة من معدات الإرسال المختلفة (وهي نفس ANTI-ESM).

ب ـ الإجراءات الدفاعية الإلكترونية : ELECTRONIC DEFENCE MEASURES

وهي عمليات وإجراءات تقليل أو منع العدو من تأثيره (التشـويش) على معداتنا المختلفة وهي نفس (ANTI-ECM).

وبما أن إستخبارات الإشارة (SIGINT) تتكون من إستخبارات الإتصالات (COMINT) والإستخبارات الإلكترونية (ELINT)، كذلك في بعض المصادر من مكـونات المضادات الإلكترونية للإجـراءات المضادة (ECCM) أمن الإشـارة (SIGSEC) والتي هذه بدورها تنقسم إلى :

أ ـ أمن الإتصالات (COMSEC) وهي كل ما يخص أمن معلومات الإتصالات من مراقبة ورصد وتحليل العدو لها، وهي تنقسم إلى:

(١) الأمن المادي (PHYSICAL SECURTY) وهو أساليب ومعدات أمن معلومات الإتصالات داخل المنشآت.

(٢) التشفير (CRYPTOSECUIRTY)

(٣) أمن الإرسال ((TRANSMISSION SECUIRTY(TRANSEC) وهو كل ما يخص أمن إرسال من أن يصل إرسالنا إلى أرض العدو، وهذا من مكوناته ((EMISSION CONTROL (EMCON) أي تقليل ما أمكن من الإرسال.

(٤) أمن الإنبعاث ((EMISSION SECUIRTY(EMSEC) وهو كل ما يخص من حفظ المعلومات من التسرب (LEAKAGE) غير المقصود، كأن تتسرب المعلومات السرية من أجهزة التشفير قبل تشفيرها على شكل إنبعاثات كهرومغناطيسية يستـطيع العـدو بمقـارنتهـا مـع الإرســال المشفـر إيجــاد مفتـاح الشفـرة (ENCRYPTION KEY)، وهذه الحماية تسمى (TEMPEST) أي قدرة الجهاز على عدم تسرب المعلومات منه عرضياً .

ب ــ الأمن الإلكتروني : ELECTRONCE SECUIRTY (ELSEC) وهو الأساليب التعبوية للحماية الإلكترونية .

ومـن أنظمة المضـادات الإلكترونية للإجراءات المضادة (ECCM) وإجـراءات الحماية الإلكترونية (E.P.M.)، استخدام أنظمة لتضاد التنصت أو التشويش المعادي منها :

أ ـ أجهزة تعمل بنظام ADAPTIVE SYSTEM

وهي أجهزة تخزن بعض الترددات أو القنوات المراد الإتصال بها فيقوم النظام بعمل الإتصال المستمر بين جهاز الإرسال وجهاز الإستقبال في الطرف الآخر لإختيار أنسب وأوضح الترددات والموجات للإتصال ويحدث هذا بطريقة آلية وسريعة.

ب ـ أجهزة تعمل بتقنية الطيف الممتد SPREAD SPECTRUM TECHNIGUES

(انظر شكل (٢ / ٢١)

ومن أنواع هذا النظام :

(١) نظام (DIRECT SEQUENCE SPREAD SPECTRUM)

وهو نظام يقوم على إرسال المعلومات بإستخدام مجال (BANDWIDTH) عريض جداً أعرض من المجال العادي ، أي بحوالي عشرات الميغا هرتز، فتكون قدرة الإرسال (TXION POWER) موزعة على كل المجال مما يصعب مراقبة ورصد العدو لهذا الإرسال وكذلك التشويش عليه .

(٢) نظام تنقل التردد (FREQUENCY HOPPING)

وهو نظام يقوم على إرسال المعلومات على التردد الحامل (FC) ويقوم هذا التردد بالتنقل السريع من تردد إلى آخر بطريقة عشوائية وسريعة مغطياً نطاق واسع من الترددات .

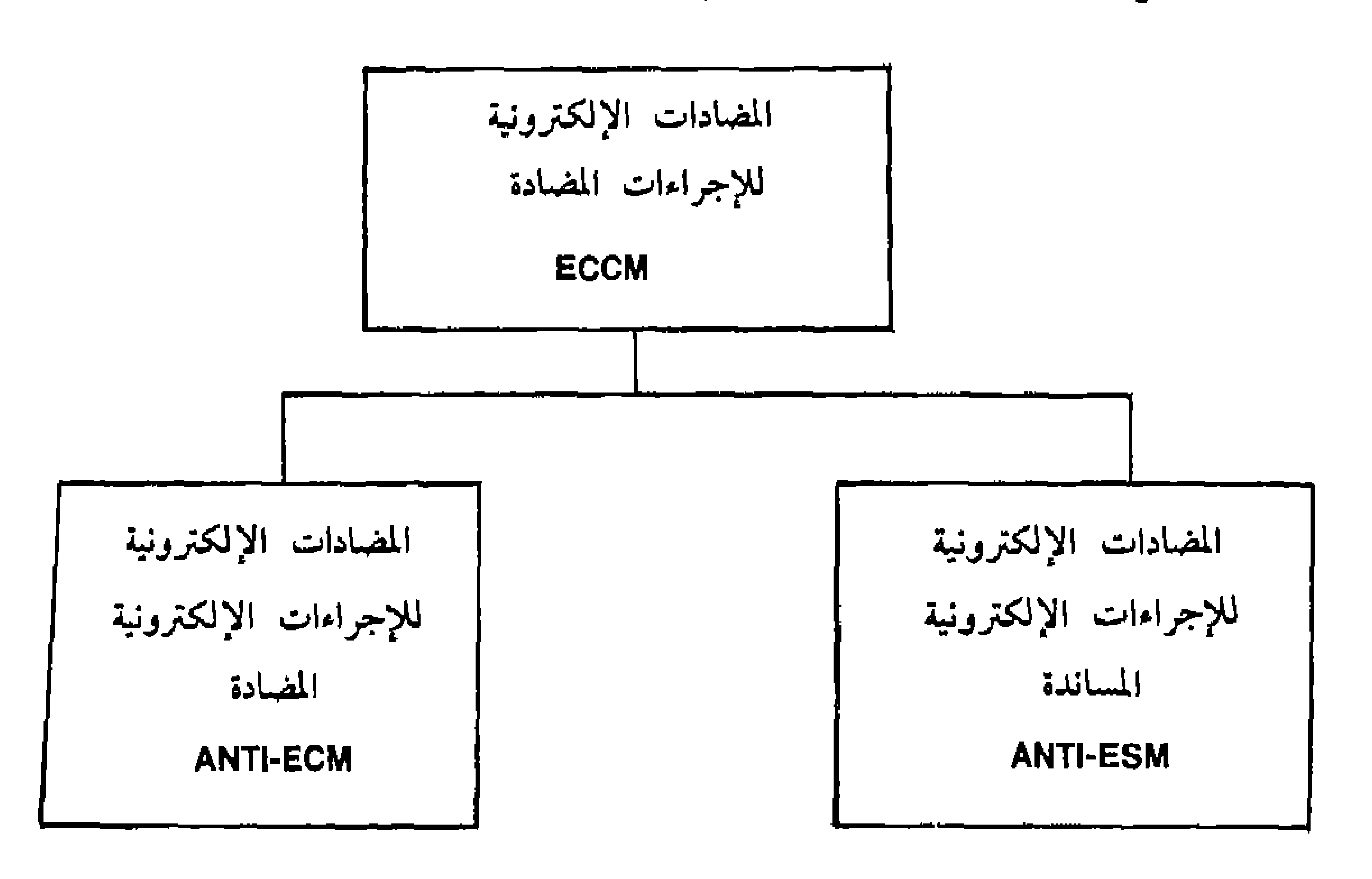
(٣) نظام تنقل الزمن (TIME HOPPING)

وهـو نظام يقـوم على إرسـال المعلومات بـطريقة سريعـة وبوقت قصـير جداً لكن بمجال عريض جداً حتى يفوت الفرصة على العدو إلتقاط هذا الإرسال ويسمى هذا النظام كذلك (BURST COMMUNICATION).

(٤) نظام (CHIRP)

وهو يستخدم في الرادارات وله نفس خواص النظام الأول ولكن بتغير مستمر بالتردد من جهة واحدة، وهو من أنواع إرسال راداري يسمى (PULSE COMPRISION).

وتتكون المضادات الإلكترونية للإجراءات المضادة من :



أ ـ المضادات الإلكترونية للإجراءات الإلكترونية المساندة (ANTI-ESM)

وهي الأجهزة الإلكترونية والأساليب الفنية التي تحمي أجهزتنا من الإجراءات الإلكترونية المساندة للعدو، ومن هذه الأساليب الفنية والأجهزة الإلكترونية الحامية :

أولاً : استعمال الكلام المشفر :

وهو أنه بقدر الإستطاعة توضع رموز معينة معروفة لكلا الطرفين للتفاهم حتى إذا حدث تنصت على هذه المكالمة لا يفهم منها شيء. وقد استخدمت هذه الفكرة منذ القدم ولكنها الآن لا تكفل الحماية الكاملة. لأن هناك أناساً متخصصين وأساتذة في علم النفس تستعين بهم الدول المتقدمة لمعرفة نفسية واضع هذه الرموز عن طريق متابعة الرموز ومن ثم محاولة فكها.

ثانياً : إستعمال أجهزة التشفير الإلكترونية :

CIPHERING OR ENCRYPTION UNIT

وهي أجهزة إلكترونية تعمل على تغيير معالم وصفات ومميزات المعلومات المراد نقلها من جهاز إلى آخر أو من مكان إلى آخر، وتكون طريقة تغيير الصفات المميزة لهذه المعلومات إما بطريقة عشوائية رتيبة أو بطريقة عشوائية غير رتيبة. فمثلاً قد يحول جهاز التشفير الإلكتروني حرف ع إلى ف فالجهاز يعمل بطريقة عشوائية رتيبة وسيحول في كل مرة حرف ع إلى ف، ولكن إذا كان جهاز التشفير الإلكتروني يعمل بطريقة عشوائية غير رتيبة فسيعمل على تغيير الحرف ع مرة إلى ف ومرة إلى ط ومرة إلى ل وهكذا وهنا نجد أن الجهاز يعمل على تغيير نفس الحرف في نفس الرسالة إلى حروف متغيرة وغير ثابتة. وطبعا جهاز التشفير عندما يعمل على تغيير صفات المعلومات بالنسبة لنا سنحسبها طريقة عشوائية (RANDOM) ولكن بالنسبة للجهاز تكون طريقة عشوائية منتظمة (PSEUDO RANDOM) ولنعلم بأن هناك عدة أنواع من المعلومات المراد نقلها سواء عن طريق التلفون أو الراديو أو الكمبيوتر أو التلكس.. الخ.

فإذا أردنا تقسيم نوعية المعلومات سنحصرها في الآتي :

١ ـ معلومات صوتية مسموعة AF:AUDIO FREQ

وهي موجات صوتية تصدر عن الإنسان أو الحيوان أو الآلات الموسيقية أو كل شيء تستطيع أذن الإنسان أن تسمعه وتتراوح ذبذبتها بين ٢٠ هرتز و ٢٠ كيلوهرتز تقريبا وتختلف من إنسان إلى آخر في دقة السمع وهي عادة غير منتظمة الطاقة والذبذبة.

٢ ـ معلومات تسمى : (ANALOGUE SIGNAL) الإشارة التناظرية :

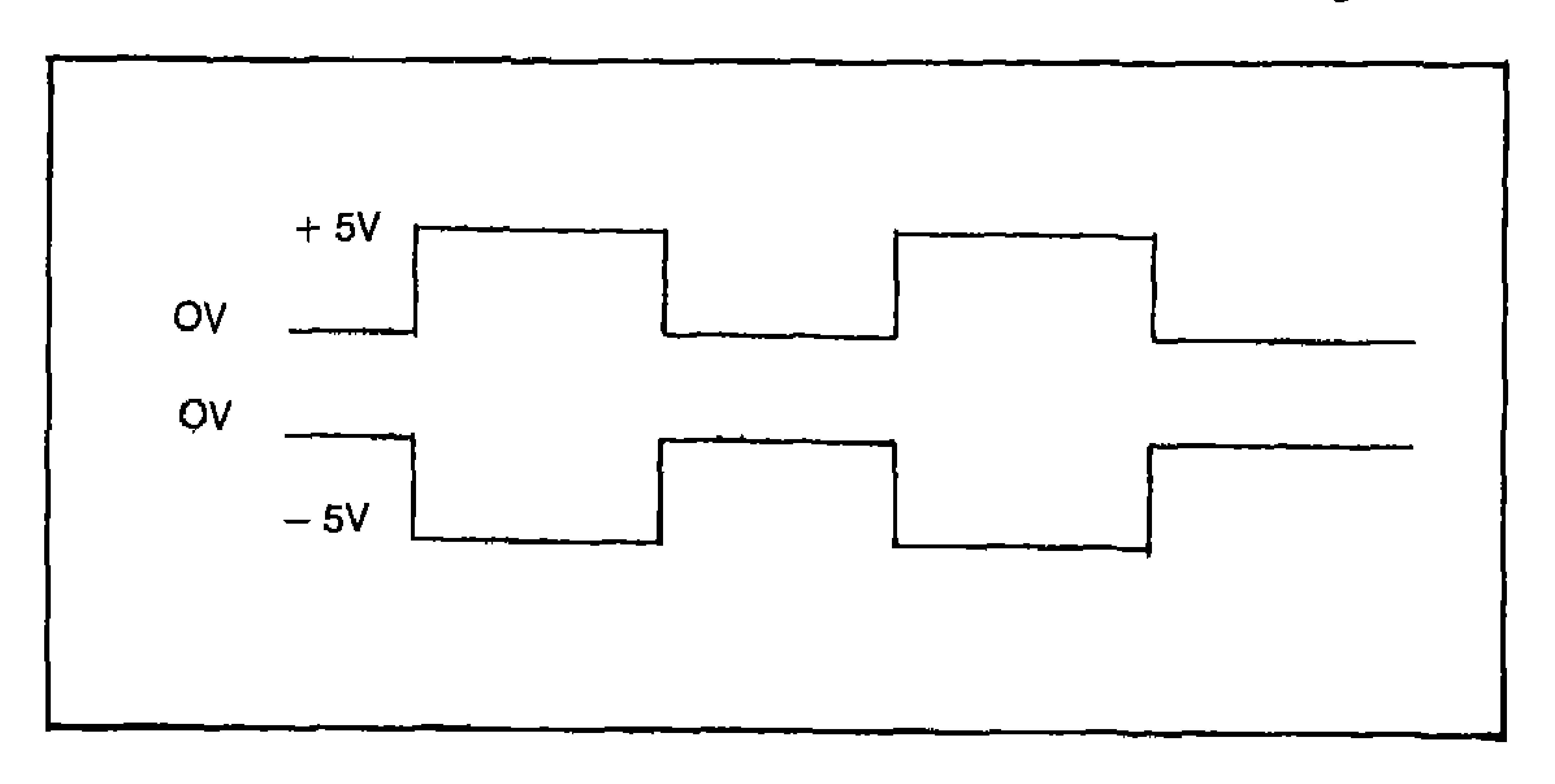
وهي المعلومات المنبعثة عن الأجهزة الكهربائية أو الأجهزة الإلكترونية أو قد تكون مسموعة أو غير مسموعة بالنسبة للإنسان وتختلف بإختلاف الأجهزة الكهربائية أو الإلكترونية مثل المعلومات الناتجة عن العدادات الكهربائية أو موجات الإتصالات. . الخ. وهي كذلك غير منتظمة الطاقة والذبذبة.

٣ ـ معلومات تسمى: (DIGITAL SIGNAL) الإشارة الرقمية :

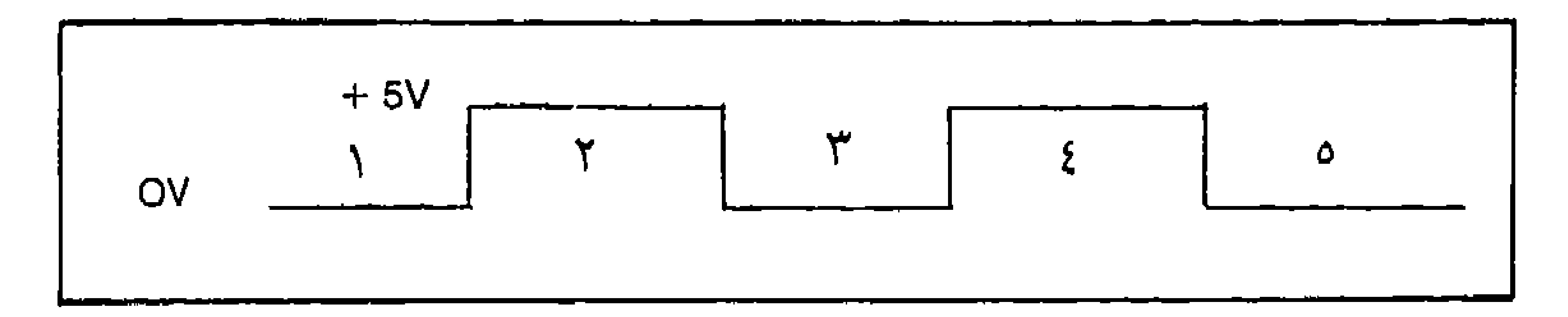
وهي تتكون من تيار كهربائي مستمر (DC VOLTAGE) عبارة عن:

أ ـ جهد كهربائي صفر (O VOLTAGE)

ب ـ جهد كهربائي + أو - ٥ ڤولت (+ 5VOLTS or -) تكون مربع معلوم الوقت أو الزمن:



وكلٍ واحدة (مربع أو وحدة زمنية) تسمى (DIGIT) وكل مجموعة من هذه تكون معلومة فمثلاً جهاز التلكس حرف ط يتكون من خمس مربعات أو وحدات زمنية (5 DIGITS).



وهكذا. . .

فبهذه الحالة نستطيع تحويل كل معلومة من المعلومات الصوتية المسمـوعة (AF) أو الإشارة التناظـرية (ANALOGUE SIGNAL) إلى كميـات معينة من الـ (DIGITS) فتكـون بعد ذلك معلومات كاملة، وهذا التحويل يتم بإستخدام دائرة تسمى (ANALOGUE TO DIGITAL CONVERTOR) ونقـل المعلومات بـإستخـدام وسط الإتصـال إمـا بـإستخـدام الكيبل (WIRE OR CABLE) كالتلفونات مثـلاً، أو استعمال الهـوائي الخارجي مثـل البث بالراديو، ويعمل جهاز التشفير على تشفير المعلومات بمفتاح إلكتروني (KEY) وهي شفرة أو رموز يجب الإتفاق عليها بين الطرفين حتى يتسنى لكل طرف في الشبكة: التشفير وفك الشفرة .

وهناك عدة أنواع من أجهزة التشفير الإلكترونية سنذكر إثنان منها حتى تدرك خاصية هذه الأجهزة.

١ ــ جهاز تشفير تناظري : ANALOGUE ENCRYPTION-(SCRAMBLER)

وهو جهاز فقط يشفر المعلومات الصوتية المسموعة (AUDIO FREQUENCY) والمعلومات التي تسمى (ANANLOGUE SIGNAL) وفكرة الجهاز هي تغيير معالم وصفات المعلومات تغيرا عشوائية في طاقة المعلومة أو ذبذبتها (.FREQ) أو وقت المعلومة. أو تغييرهما جميعا: (2 DIMENSIONS) وهو جهاز تشفير بسيط عادة يستعمل من قبل الأماكن غير شديدة الأهمية.

وتقوم فكرة هذا الجهاز على تحويل المعلومات الصوتية المسموعة .AUDIO FREQ)

(ANALOGUE SIGNAL) إلى معلومات (DIGITAL DATA) بدائرة تسمى (ANALOGUE TO DIGITAL CONVERTOR) ثم ترتيبها على شكل (ADDRESSES) كثيرة ثم أخذ هذه الـ (ADDRESSES) بطريقة عشوائية رتيبة أو غير رتيبة وإرسالها آلياً للجهاز المراد نقل المعلومات إليه، وعند الطرف الآخر المستقبل للمعلومات المشفرة سيعمل جهاز التشفير هذا على فك الشفرة بنفس المفتاح المتفق عليه بين الطرفين فيعمل بإستعمال هذا المفتاح الإلكتروني على تجميع الـ (ADDRESSES) ثم ترتيبها لكي يرسلها إلى دائرة (DIGITAL ANALOGUE CONVERTOR) وبالتالي نستطيع فهم المعلومات.

وأن هذه النوعية من أجهزة التشفير تحتاج مراقبتها وفك تشفيرها إلى معرفة مفتاح الشفرة واستعمال جهاز كمبيوتر وهذا الموضوع من أصعب مواضيع الحرب الإلكترونية .

٢ ـ جهاز تشفير رقمي : DIGITAL ENCRYPTION

وهو من أقوى أجهزة التشفير وأدقها وأصعبها فكا للشفرة إذ يحتاج إلى معرفة مفتاح الشفرة وأجهزة كمبيوتر ضخمة جداً ووقت طويل حتى يمكن معرفة المعلومات المرسلة، وهذا الوقت قد يصل إلى سنوات من التحليل المتواصل. ويجب إدخال المعلومات في الجهاز على شكل (DIGITAL DATA) فقط باستعمال (ANALOGUE TO DIGITAL CONVERTOR) ويعمل بنفس طريقة الجهاز السابق بالإضافة إلى أنه يبدل تشفير (ADDRESSES) عشوائيا ، فهذا الجهاز يعمل على تشفير كل (DIGIT) أي تشفير (BIT BY BIT) وهذه الأجهزة تستعمل لنقل المعلومات المهمة جداً.

وسنذكر هنا نوعية من أجهزة التشفير التي تركب على أجهزة الإرسال والإستقبال.

١ ـ أجهزة تشفير لأطراف الإتصال : END TO END CIPHERING

وهي أن يركب جهاز تشفير في كل طرف من الإتصال أي عند المرسل المتكلم والمستقبل السامع ويسمى كذلك : (TERMINAL CIPHERING UNIT)

٢ ـ أجهزة تشفير لمحطات الإتصال :

وهي أن تركب أجهزة التشفير في كل محطة من محطات الإتصال أي عند محطة الإرسال وعند محطة الإستقبال، فجهاز التشفير يركب في مقسم التلفونات فيشفر كل الخطوط أو بعضها في المقسم (EXCHANGE) وعند مقسم الإستقبال يفك جهاز التشفير

جميع أو بعض المكالمات الآتية من خارج المقسم، ويسمى هذا النوع من أجهزة التشفير (BULK ENCRYPTION UNIT) وهي كذلك تستخدم لتشفير أجهزة الإتصالات المتعددة القنوات (MULTICHANNEL RADIO) وبهذه النوعية من الأجهزة نستطيع حماية أجهزتنا من المراقبة والتحليل.

ويمكن تركيب أجهزة التشفير لجميع وسائل الإتصالات مثل :

أ ـ الأجهزة الصوتية (VOICE EQUIPMENTS) مثل أجهزة الهاتف والراديو.
ب ـ أجهزة نقل الصورة الفاكسميل (FAXIMILE).
جـ ـ أجهزة نقل الرسائل (TEXT) مثل أجهزة التلكس و (TTY).
د ـ أجهزة نقل البيانات (DATA) لنقل بيانات ومعلومات بين أجهزة الكمبيوتر.
هـ ـ أجهزة نقل معلومات مختلفة النوعية بإستخدام أجهزة إتصالات متعددة القنوات (MULTICHANNEL).

ويمكن تقسيم أجهزة التشفير حسب تقنية التشفير كالآتي :
أ ـ أجهزة التشفير التناظرية (ANALOGUE ENCRYPTION) ويمكن تقسيمها كالآتي :
١ ـ تشفير يعمل بطريقة (INVERTER) أي بعكس مجال التردد.
٢ ـ تشفير يعمل بطريقة البعد الواحد (ONE DIMENSION) وهو لخبطة بُعد واحد إما بُعد الزمن أو بُعد التردد.
٣ ـ تشفير يعمل بطريقة البعدين (TWO DIMENSIONS) وهو لخبطة بُعد الزمن وبُعد التردد، وهو أحسن أنواع التشفير هذه وأكثرها سرية.

ب ـ أجهزة التشفير الرقمية (DIGITAL ENCRYPTION) ويمكن تقسيمها كالآتي :
١ ـ تشفير يعمل بطريقة تشفير مجموعة / مجموعة (BLOCK BY BLOCK CIPHERING). أي تشفير مجموعة أرقام أو أحرف ثم المجموعة التالية وهكذا.
٢ ـ تشفير يعمل بطريقة (KEY STREAM CIPHERING). أي بتشفير مستمر لكل المعلومات بسيل من مفتاح الشفرة يمزج بالمعلومات بصورة مستمرة.

كما يجب لفت النظر إلى أن هناك نقاط يجب أخذها بعين الإعتبار عند إختيار جهاز التشفير من هذه النقاط.
أ ـ نوعية المعلومات المراد إرسالها (معلومات عادية ـ محظورة ـ سرية ـ سرية للغاية).

ب ـ تحديد الجهة المراد حماية المعلومات عنها، هل نحن نريد المحافظة على سرية معلوماتنا ضد رجل الشارع العادي أم ضد هواة الراديو أم ضد الأرهابيين والعصابات المنظمة أم ضد الدول المجاورة أم ضد الدول العظمى.

جـ ـ كذلك يجب تحديد مدى صلاحية المعلومات عندما تفك شفرتها من قبل العدو هل ستكون ذات أهمية بعد ساعة من إرسالها وفك شفرتها أو يوم أو شهر وهكذا .

ومن هذه النقاط نستطيع إختيار التشفير المناسب لإحتياجنا حسب الإستخدام.

كما يجب أن نعلم أن علم التشفير ينقسم إلى قسمين :

أ ـ علم عمل التشفير (CRYPTOGRAPHY) وهو علم طرق وتقنيات التشفير.

ب ـ علم تحليل التشفير (CRYPTOANALYSIS) وهو علم طرق فك وتحليل التشفير.

ومن متطلبات كسر أو فك أو تحليل الشفرة أو التشفير يجب معرفة الآتي :

أ ـ أسلوب عمل جهاز التشفير ويسمى (ALGORITHM) وهو طريقة عمل جهاز التشفير لإخراج (KEY STREAM) الذي يمزج مع المعلومات المراد تشفيرها فينتج معلومات مشفرة، ويسمى كذلك جهاز أو دائرة انتاج مفتاح الشفرة (KEY GENERATOR) ، وهذا عادة معروف لدى الجهات التي تهتم بفك الشفرات.

ب ـ مفتاح الشفرة (ENCRYPTION KEY) وهو أهم شيء في أجهزة التشفير إذ بتسرب مفتاح الشفرة (ومعرفة ALGORITHM) ممكن برمجة أجهزة الكمبيوتر ومحاولة فك الشفرة .

وهناك عدة أنواع من مفاتيح الشفرة تدخل في جهاز التشفير منها :

١ ـ مفتاح شفرة الإتصالات (COMMUNICATION KEY) :-

وهو يدخل في جهاز التشفير مباشرة عن طريق مفاتيح التحكم الأمامية لجهاز التشفير وهذا المفتاح يتغير بصورة دورية.

٢ ـ مفتاح التزامن (SYNCHRONIZATION KEY) : -

وهو يختار ويوضع بطريقة آلية داخل الجهاز.

٣ ـ المفتاح الأساسي (STRUCTURE KEY) :-

وهو مفتاح يوضع داخل الجهاز عن طريق دائرة كهربائية صغيرة (EPROM CHIP).

٤ ـ مفتاح العميل (CUSTOMER KEY) : ـ

وهو مفتاح يوضع لمرة واحدة من قبل مصنع أجهزة التشفير إذ لكل عميل أو دولة مفتاح شفرة خاص .

وجميع هذه المفاتيح مجتمعة تكون بما يسمى مفتاح الشفرة لينتج بما يسمى (KEY STREAM).

وهناك شيء يسمى إدارة مفتاح الشفرة (KEY MANAGMENT) يجب الإهتمام بها حتى نحافظ على أهم شيء في أجهزة التشفير، وهذه الإدارة تقوم على الخطوات أو النقاط التالية :

أ ـــ إنتاج مفتاح الشفرة (KEY GENERATION) وهي طريقة إختيار مفتاح الشفرة .
ب ـــ تخزين مفتاح الشفرة (KEY STORAGE) وهي طريقة حفظ مفتاح الشفرة.
جـ ـــ توثيق مفتاح الشفرة (KEY VERIFICATION) وهي طريقة التأكد من إدخال مفتاح الشفرة الصحيح بصورة صحيحة لكل المشتركين.
د ـــ توزيع مفتاح الشفرة (KEY DISTRIBUTION) وهي كيفية توزيع مفاتيح الشفرة للمشتركين بصورة سرية وسريعة وأمينة.

هـ ـــ تدمير مفتاح الشفرة (KEY DESTRUCTION) وهي طريقة التخلص من مفتاح الشفرة بصورة مضمونة وسريعة وأكيدة.

كما يجب أن نلفت الإنتباه أن جميع أو معظم الدول التي لديها شركات تصنع أجهزة تشفير لا تسمح بتصدير أجهزة التشفير لدول أخرى حتى تستطيع هذه الدول من خلال مؤسساتها ومعاهدها المعنية أن :

أ ـــ التأكد من أن أجهزة التشفير هذه جيدة ومطابقة لأصول التشفير.
ب ـــ معرفة كل ما يخص أسلوب وتقنية تشفير هذه الأجهزة (ALGORITHIM) و (KEY GENERATOR) وما هي أبسط وأسرع طرق فك شفرتها.
جـ ـــ أن تكون أجهزة التشفير هذه المراد تصديرها ليست بمستوى وقدرة وكفاءة مثيلتها المستخدمة لدى الدولة نفسها.

ونضرب مثالا على ذلك، في الولايات المتحدة يقوم بهذا العمل وكالة الأمن القومي (NATIONAL SECUIRTY AGENCY « N.S.A.) .

هذا بالنسبة للشركات والدول المصنعة لأجهزة التشفير، أما بالنسبة للدول التي تشتري وتستخدم أجهزة التشفير فمن الممكن إختبار وفحص قدرة وجودة ومعرفة مستوى أجهزة التشفير التي لديها من خلال الإتصال بمعهد متخصص في ألمانيا الغربية بالرياضيات وعلم التشفير يقوم بتقييم هذه الأجهزة وإعطاء النتائج.

وكما قلنا فإن من أصعب عمليات الحرب الإلكترونية فك الشفرات وخاصة الكلام أو المعلومات (DATA) المشفرة إلكترونيا أي بأجهزة تشفير إلكترونية، وكلما كانت أجهزة التشفير الإلكترونية معقدة كان ذلك التشفير أكثر صعوبة واحتجنا أجهزة كمبيوتر أكبر وأسرع لعمليات الفك هذه.

وسنورد هنا بعض الوقائع التي حدثت في السابق بشأن عملية فك التشفير الإلكتروني :

١ ـ في الحرب العالمية الثانية استطاعت القوات الأمريكية إلتقاط الشفرة اليابانية المستخدمة بين القوات اليابانية في المحيط الهادي والمتعلقة بعملية الهجوم الياباني بالطائرات القاذفة اليابانية على ميناء بيرل هاربر الأمريكي في جزر هاواي واستطاعو فك التشفير قبل فوات الأوان، لكن الأمريكيون الذين قاموا بعملية الفك لم يصلوا إلى المعنى الحقيقي في الشفرة إذ كانت تتكون أصلا من شفرتين (تشفير مضاعف) أي معلومات مشفرة ثم تشفير المعلومات المشفرة.

٢ ـ في حرب فوكلاند عام ١٩٨٢ استطاع الأمريكيون الحصول على معلومات مشفرة بين القوات الأرجنتينية وبعد أن فك الأمريكيون التشفير، أبلغو الإنجليز (الذين هم خصم الأرجنتين في تلك الحرب) فاستخدموا بدورهم تلك المعلومات في الحرب، فساعدتهم في تحقيق انتصارات عديدة، وقد قيل أنه لو لم يحصل الإنجليز على تلك المعلومات لطال أمد الحرب ولما تغلب الإنجليز على الأرجنتين بهذه السهولة..

٣ ـ في سبتمبر عام ١٩٨٣ استطاعت وسائل الإستطلاع الأمريكية الإلكترونية (SIGINT) التقاط الأوامر (المشفرة) بين القيادة السوفياتية ووسائل الدفاع السوفيتية والتي تحمل أمر مهاجمة طائرة الخطوط الجوية الكورية البوينغ ٧٤٧ المنحرفة عن مسارها في شمال شرق آسيا، وقد بعث الأمريكيون تلك المعلومات المشفرة إلى مركز فك التشفير في الولايات المتحدة الأمريكية لفك الشفرة ومعرفة ما

تحويه من معلومات واستطاعوا بعد أربع ساعات فك الشفرة لكن بعد فوات الأوان، إذ في غضون ذلك هاجمت وسائل الدفاع السوفيتية الطائرة المدنية الكورية وأسقطتها.

ثالثاً : استعمال أقل قوة إرسال :

وهي عمل دراسة لتحديد أقل قوة من الإرسال (في الراديو) نستطيع بها الاتصال، إذ أن القوة أو الطاقة الزائدة عن الحاجة سوف تنقل المعلومات والإتصالات إلى مناطق العدو.

رابعاً : استعمال أقل وقت للإرسال :

فيجب أن يتم الإرسال عند الحاجة فقط وبشكل مختصر لأن طول وقت الإرسال يعطي العدو فرصة أكبر للمراقبة والتحليل وتحديد موقع الإتصال عن طريق موجد الإتجاه.

خامساً : استعمال كيبلات بدل الهوائيات للإتصالات ما أمكن لأن الهوائيات قد تعمل على بث المعلومات إلى أماكن العدو وتتعرض للمراقبة والتنصت والتحليل.

سادساً : استعمال هوائيات موجهة DIRECTIONAL ANTENNA

وهذا تستعمل فقط في حالة ما إذا أريد الإتصال بجهة معينة، إذ أن استخدام هذا النوع من الهوائيات يقلل من فرصة المراقبة والتنصت. وهذه الهوائيات يجب أن تستعمل خاصة عند الحدود.

سابعاً : استخدام أكبر عدد ممكن من التضمينات مثل (FM, AM, USB, LSB,) لأننا كلما نوعنا في استخدام هذا التضمين جعلنا مراقبة العدو لموجاتنا مهمة صعبة.

ثامناً : محاولة استعمال موجات أو ذبذبة خاصة في حالة الطوارىء، وهذا من شأنه أن يقلل من فرصة مراقبة المعلومات المرسلة في أثناء الطوارىء، خاصة وأنه أثناء الطوارىء لا تتبع أصول الإرسال بدقة.

تاسعاً : استعمال مجالات الذبذبات غير المعروفة مثلاً: استعمال ذبذبات للإتصالات فوق ١٠٠٠ ميغا هرتز أو استعمال ذبذبات للرادارات فوق ٢٠٠٠٠ ميغا هرتز.

عاشراً : استخدام الذبذبة المتعانقة أو القريبة (HUGGING OR ADJUSNT FREQUENCY) وهي تعمد الإرسال بذبذبة قريبة جداً من ذبذبة العدو لأنه لا يتنصت على ذبذباته وحتى يتردد في التشويش عليها لأنه بذلك قد يؤثر على ذبذبته أيضاً.

حادي عشر : وضع أجهزة الإرسال وخاصة أجهزة الترددات الأعلى من ٣٠ ميغا هرتز في موضع يصعب على العدو التقاط الإرساليات منه كأن يوضع الهوائي خلف مبنى أو جبل أو ما شابه ذلك.

ثاني عشر : استخدام طريقة السيطرة على الإشعاع (EMISSION CONTROL). وهي إجراء دراسة وافية لجميع الموجات الكهرومغناطيسية المنبعثة من أراضينا لعمل سيطرة بهدف تقليل هذه الإنبعاثات حتى لا يحصل العدو على المعلومات التي تتضمنها.

ب ـ المضادات الإلكترونية للإجراءات الإلكترونية المضادة (ANTI-ECM)

وهي العمليات التي تستخدم فيها الأجهزة الإلكترونية والأساليب الفنية التي تحمي أجهزتنا من الإجراءات الإلكترونية المضادة للعدو.

وهي التي تحمي أجهزتنا من التشويش عليها أو إعاقتها أو مخادعتها ومن هذه الأجهزة والأساليب:

١ ـ استعمال أجهزة عالية التشفير لتفادي التشويش المخادع.

٢ ـ استعمال أكبر عدد ممكن من مجالات الذبذبات مثلاً (VLF, LF, MF, HF, VHF, UHF, SHF) مما يتيح مجالا للإتصال من خلال مجال أو أكثر لم يشوش عيه من قبل العدو مهما كان حجم تشويشه، ذلك لأنه من الصعوبة التشويش على جميع مجالات الذبذبات في وقت واحد.

٣ ـ استعمال أجهزة (FREQ. HOPPING) تنقل التردد[1] وكما أن هذه الأجهزة تحمي إتصالاتنا من التنصت والمراقبة فهي كذلك تحميها نسبيا من التشويش الحاجب والتشويش المخادع. إذ تعمل أجهزة تنقل التردد على تنقل الذبذبة الحاملة (CAR-PIER FREQUENCY) من مكان لأخر وهذا التنقل يكون سريعا لدرجة تصل إلى ١٠٠٠ مرة في الثانية، والتنقل من ذبذبة لأخرى يكون في نطاق قد يصل إلى ٣٠ ميغاهرتز، ولكن يقال أن التشويش على ٣٠٪ فقط من المجال أو النطاق المرسل يكفي لتعمية هذه النوعية من الإتصالات.

٤ ـ كذلك يوجد ضمن أجهزة الرادار المتطورة أجهزة تحمل نفس الفكرة السابقة ولكن بسرعة أقل في التنقل وبنطاق أعرض بكثير، إذ يصل نطاق التنقل في بعض الأجهزة إلى ١٠٠ ميغا هرتز وتسمى هذه الطريقة (FREQ. AGILITY).

٥ ـ إستعمال أجهزة (SPREAD SPECTRUM) وهي طريقة تستعمل كما قلنا مجالا أو نطاقا عريضا جدا من الذبذبات لنقل المعلومات يصعب على جهاز التشويش

---

(١) للتردد المتنقل ثلاث معدلات:

أ ـ التردد المتنقل ذو المعدل البطيء SLOW RATE وهو حوالي ٨ نقلات في الثانية.

ب ـ التردد المتنقل ذو المعدل المتوسط MIDUMRATE وهو حوالي ٣٠٠ نقلة في الثانية.

جـ ـ التردد المتنقل ذو المعدل السريع HIGH RATE وهو حوالي ١٠٠٠ نقلة في الثانية.

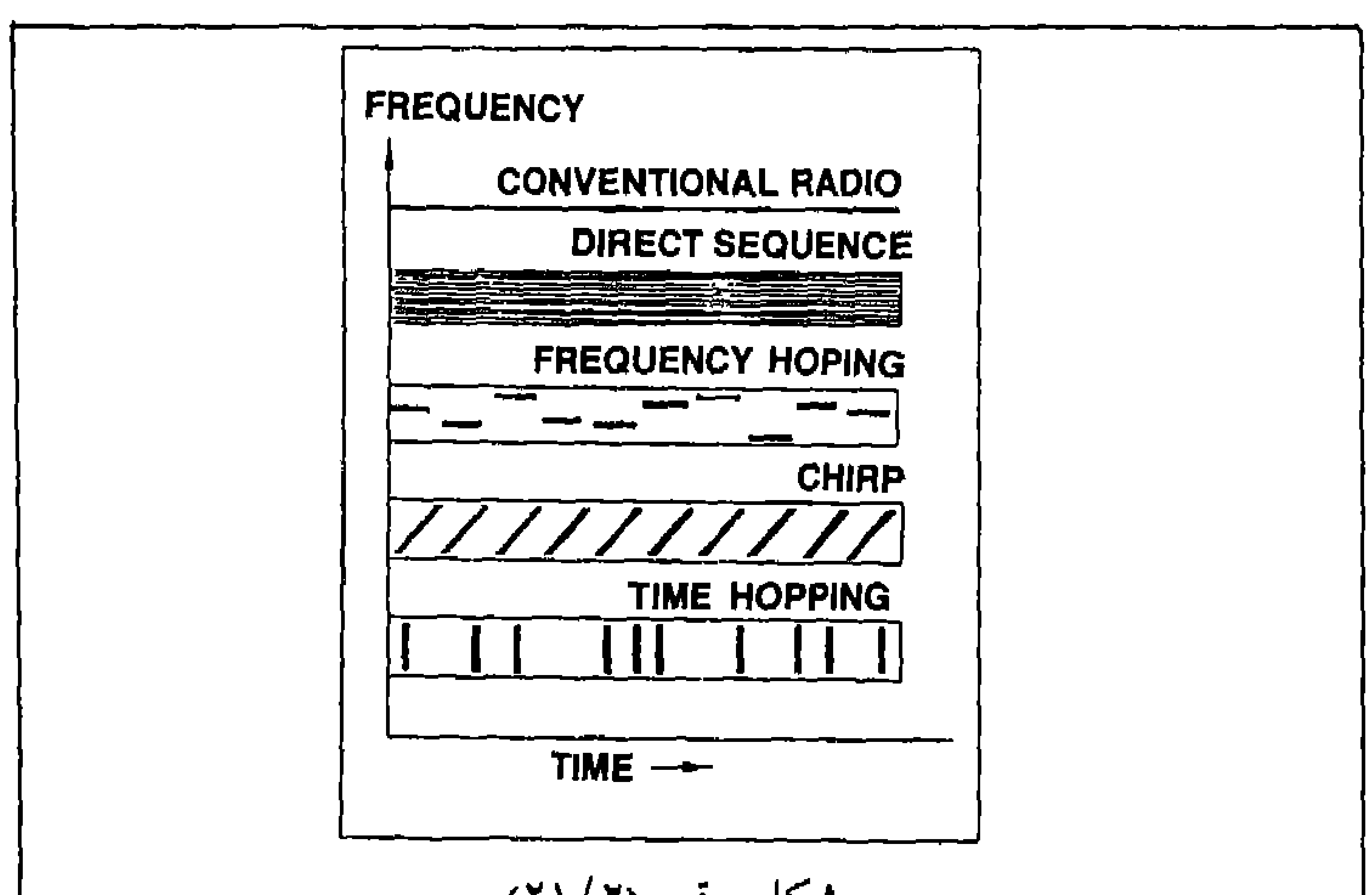
تغطيته أو إرسال طاقة تشويش أعلى من طاقة المعلومات المرسلة .

٦ ـ وضع أجهزة الإستقبال في أماكن يصعب على العدو توجيه موجات التشويش نحوها كأن تكون خلف جبل أو تل أو بناء كبير.

٧ ـ استخدام صواريخ مضادة لأجهزة التشويش تعمل بطريقة : (H.O.J- HOME ON JAMMING) إذ تتجه هذه الصواريخ نحو جهاز التشويش وحده.

٨ ـ وضع عدة أجهزة إتصال متنوعة التردد مثل (M, H,F VH,F UHF) عند كل نقطة اتصال حتى إذا حدث تشويش على أحدها يمكن الاستمرار بنفس الموجه المشوشة عليها، مستخدماً في نفس الوقت جهاز آخر لـه تردد مختلف تـرسل بـه المعلومات المراد إرسالها (وتسمى هذه طريقة الإنتشار DEPLOYMENT) .

٩ ـ تحديد موجات أو ذبذبات خاصة تستخدم في حالات التشويش فقط دون استخدامها في الحالات العادية، حتى يتوفر فيها عنصر المفاجأة للعدو.



شكل رقم (٢/٢١)

الشكل يبين أنواع وأنظمة (SPREAD SPECTRUM) مقارنة مع نظام الإرسال اللاسلكي العادي .

الباب الثالث

طائرات الانذار المبكر والحرب الالكترونية

١ ـ طائرات الإنذار المبكر

AEW - AIRBORNE EARLY WARNING

طائرات الإنذار المبكر هي الطائرات التي تحمل رادارات ذات مدى بعيد والرادار في هذه الطائرات هو قلبها النابض وعليه (أي الرادار) أن يكون دقيقا في التقاط الأهداف مهما كانت درجة ارتفاعها أو إنخفاضها حتى أن بعض الرادارات تعطي معلومات عن أهداف ضئيلة الحجم ـ كقارب صغير ذي سرعة محدودة مثلاً ـ حتى ولو كانت تبعد عن هذه الأهداف بمسافة تزيد على مائة كيلومتر.

بدأت الدولتان العظيمتان في التفكير وعمل طائرات إنذار مبكر في أوائل الستينات، وبعد مضي سنوات قليلة كانت طائرات التجربة تحلق معطية نتائج باهرة.

ثم تطور الأمر بعد ذلك إلى تزويد الطائرات برادارات أخرى تلتقط إرسال الأجهزة عن بعد كبير وتحدد مواقعها وهو ما يعرف بالرادار السلبي (PASSIVE RADAR) كما زودت بأجهزة مميزة للأهداف الصديقة أو المعادية (IFF: IDENTIFICATION FRIEND OR FOE) بواسطة شفرات معينة ترسل في الهواء.

وطائرات الإنذار المبكر عادة إما أن تكون مصممة للكشف فوق اليابسة أو فوق الماء أو كلاهما.

وكان يراعى في هذه الطائرات عند اختيارها لتكون طائرات إنذار مبكر أن تكون كبيرة الحجم كالطائرات التجارية المدنية، والمثال على ذلك طائرة الأواكس الأمريكية أو الأواكس الروسية (MOSS).

ثم بعد ذلك وضعت فيها أجهزة (ECCM) لحمايتها من التشويش المعادي.

وأجهزة (ESM) لمراقبة الرادارات الأرضية والجوية وكذلك الإتصالات اللاسلكية.

والبعض من هذه الطائرات يوجد بها أجهزة تشويش (ECM) لحمايتها من الصواريخ الموجهة إليها.

كما يوجد بهذا النوع من الطائرات أجهزة ملاحية (NAVIGATIONAL AIDS) تعطي معلومات دقيقة جدا لملاحيهـا عن موقعها وتحديد مكانها.

ولكل من هذه الأجهزة طاقم للكشف الراداري والمراقبة وتحليل المعلومات الملتقطة لتوجيه الأسلحة الأخرى من طائرات مقاتلة، وسفن حربية، وغواصات، أو قوات برية أو دفاع جوي.

كما ترسل طائرات الإنذار المبكر كل المعلومات التي تحصل عليها إلى غرفة العمليات الأرضية أو الجوية لإتخاذ الإجراءات المناسبة.

ونشأت فكرة هذه الطائرات أصلاً بناء على رغبة من خبراء جيوش الدولتين العظميين لحل مشكلة الإنذار المبكر الأرضي الذي اتضح أن له نقاط ضعف أهمها: عدم القدرة على الكشف عن الأهداف البعيدة (كالطائرات المنخفضة جداً FLYING LO-LO- LO) حتى تعطي طائرات الإنذار المبكر الجيوش وقت إنذار أكبر لإتخاذ الإجراءات المناسبة قبل فوات الأوان.

ومما يجدر ذكره ان الإنذار والكشف وظيفتان مستقلتان عن بعضهما فمعدات الإنذار تعمل على تلافي المفاجآت التكتيكية في الميدان، بينما تقوم معدات الكشف بالتبليغ عن حدوث الهجوم أو إحتمالات الهجوم، ومدى قرب القوات المعادية، ومكان وجودها، وحجمها، ونوع نشاطها، وأسلحتها.

ولكن وظيفة الإنذار أعم، إذ أنها تشمل إجراءات الكشف بالإضافة إلى عملية إتخاذ القرارات المناسبة بعد تلقي المعلومات من مختلف أنواع الأجهزة الإلكترونية وتحليلها.(١)

---

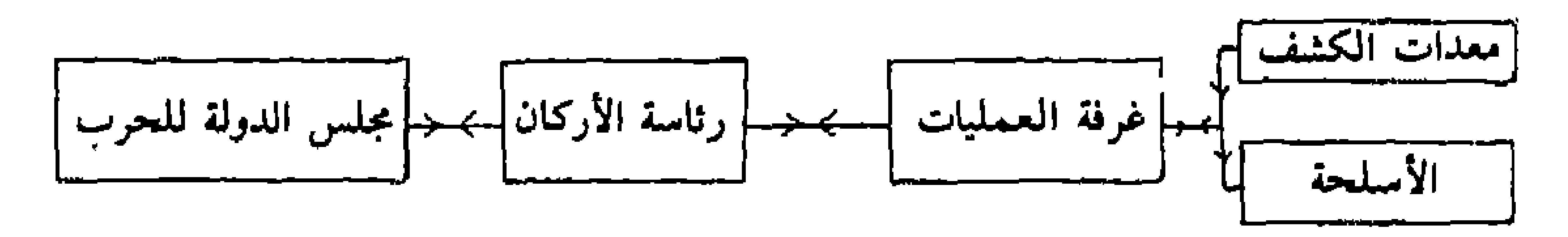
(١) راجع الموسوعة العسكرية طبعة ١٩٧٧م المؤسسة العربية للدراسات والنشرة ص ٥٣٠.

٢ ـ نظام القيادة والسيطرة والإتصالات

C³, COMMAND, CONTROL AND COMMUNICATIONS

وهو مركز إما لكل قوات الدولة (البرية والجوية والبحرية) أو لكل قوة منها على حدة ويعمل هذا المركز بإستخدام الأجهزة المختلفة وبإستعمال العقول الإلكترونية فيستقبل المعلومات من أجهزة الكشف المختلفة ويتناولها بالتنسيق والتحليل بحساب دقيق لتحديد أماكن النشاط المعادي ولمعرفة نوع هذا النشاط وإتجاهه.

وبعمليات تحويل معلومات ومعطيات أنظمة الكشف والإنذار إلى بيانات واضحة، يتحدد الموقف ويتم إختيار نوعية وطبيعة السلاح أو المعدات التي ينبغي استخدامها ضد النشاطات المعادية بأنواعها، وذلك تبعا لخطط الدولة في الهجوم والدفاع، وكل هذه الإجراءات تتم باستخدام«الإتصالات»، وهو القلب النابض، إذ بدونه لن تكون هناك قيادة ولا سيطرة[1].



وبهذا الشكل نرى أن معدات الكشف والإنذار تصب معلوماتها الحالية في غرفة العمليات لتحليلها وتقويمها لتحديد الموقف، ومن ثم رفع خلاصة الموقف إلى الجهات التي تصنع القرار (DECISION MAKERS) وهي رئاسة الأركان ومجلس الدولة للحرب، ويكون القرار النهائي هنا للدولة، حيث تكون قد نوقشت فيه جميع الجوانب السياسية والإقتصادية والدولية.. الخ، ليعود بعد ذلك القرار النهائي إلى غرفة العمليات التي تصدر الأوامر إلى أنظمة السلاح لإتخاذ اللازم.

وكلما كانت أساليب نقل المعلومات والمداولات سهلة وميسرة وسرية وسريعة، كان نظام القيادة والسيطرة والإتصالات(C³) عالي الكفاءة والأداء وبالتالي ترتفع كفاءة العمليات الحربية للدولة،ولهذا دائما يطلق على نظام القيادة والسيطرةوالإتصالات(C³)

(١) المصدر السابق، ومجلة INTERNATIONAL DEFENCE REVIEW عدد خاص عن MILITARY ELECTRONICS عام ١٩٨٠ صفحة ٣٠.

العالي الكفاءة نظام « السلاح المضاعف » (FORCE MULTIPLIER OR FORCE INTENSIFIER)[1]

هذا في حالة التوتر أو الحرب ، أما في حالة السلم فلكل قسم من هذا النظام أوامر وأساليب يتبعها وتسمى هذه الأوامر (STANDARD OPERATIONS PROCED-URE « SOP ») وهذا النظام (C^3) أو كما يطلق عليه أيضا اسم « الإدارة الحربية» (WAR MANAGMENT) يجب أن يتحلى بمزايا عديدة أهمها :

أ ـ أن يكون شديد الدقة.

ب ـ سريع الإجراء.

جـ ـ عالي الكفاءة.

هذا لكي تكون إجراءاته من :

كشف ← وتقويم ← ورد فعل في الوقت المناسب.

كذلك يجب أن تتوفر عوامل عديدة لنجاح هذا النظام منها :

أ ـ الأخذ بالمعلومات المستقاة من معدات الكشف بجدية لأنها هي الأقرب لنشاطات العدو.

ب ـ وضع معدات ذات كشف بعيد المدى، لكي نحصل على وقت كاف لإتخاذ القرار.

جـ ـ التدريب المتواصل لأفراد النظام.

د ـ وضع ضباط ذوي كفاءة عالية في هذا النظام لكي لا نعتمد على أجهزة الكشف والكمبيوتر إعتماداً كاملاً لأن تلك المعدات لن تتحمل المسؤولية أو المساءلة عند حدوث أخطاء.

هـ ـ إعطاء أصحاب القرار الوقت الكافي لإتخاذ القرار الصائب بدون إعطائهم معلومات كثيرة تكون مدعاة للحيرة والتردد.

و ـ إعطاء وتوصيل أوامر واضحة للأسلحة لإطلاق النار أو تقييدها.

ز ـ معرفة نتائج إطلاق النيران أولا بأول.

ح ـ أن يكون النظام ذو قابلية كبيرة في إعادة ترتيب صفوفه عند وقوع هجوم أو مفاجآت، وأن تكون هناك معدات وأسلحة احتياطية.

---

(١) مجلة MILITARY TECHNOLOGY عدد مارس ١٩٨٤ صفحة ٢٠.

وكما ذكرنا في الأساس الثالث في الباب الثاني إذا كان التشويش مركزا على قيادة العدو وسيطرته وإتصالاته، فإن هذا من شأنه تقليل فعالية قواته وعملياته بشكل ملحوظ ومؤثر، وهذا النوع من التشويش على هذا النظام يطلق عليه الإجراءات المضادة للقيادة والسيطرة والإتصالات .

(C³CM: COMMAND, CONTROL COMMUNLATIONSCOUNTER MEASURES) لذلك نرى أن حلف الناتو من فرط اهتمامه بنظام القيادة والسيطرة والإتصالات يخصص ٤٠٪[١] من نفقاته العسكرية العامة لهذا النظام.

وهناك أيضا نظام يطلق عليه اسم القيادة والسيطرة والإتصالات والإستخبارات (C³I: COMMAND, CONTROL, COMMUNICATION AND INTELLIGENCE) وهو شبيه بالنظام السابق مضافاً إليه معلومات الإستخبارات بأنواعها وخاصة الإستخبارات الإلكترونية (SIGINT) ، والإجراءات الإلكترونية المساندة (ESM) التي تساهم في تحديد الموقف والإجراءات الدفاعية أو الهجومية بشكل أكثر دقة وفعالية.

وثم نظام آخر يطلق عليه اسم القيادة والسيطرة والإتصالات والإجراءات الإلكترونية المضادة (EC⁴: ELECTRONIC COMMAND, CONTROL, COMMUNICATION AND COUNTER-MEASURES) وهو يشبه إلى حد كبير نظام القيادة والسيطرة والإتصالات ولكنه يتميز بتركيز أعظم نحو استخدام أجهزة الحرب الإلكترونية والإعتماد عليها في إدارة أسلحة ومعدات الجيش هجوميا ودفاعياً، وخاصة الإعتماد على تأثيرات التشويش والمخادعة الإلكترونية[٢].

وقد تكون طائرات الإنذار المبكر نظاما مصغرا للقيادة والسيطرة والإتصالات[٣] وذلك لما فيها من الأجهزة والمعدات الكافية، ولو لفترة معينة من الوقت. كما أنها تعتبر أكثر بقاء من مراكز العمليات الأرضية وخاصة عند حدوث حرب نووية.

وقد لاقت فكرة طائرات الإنذار المبكر استحسانا من بعض الأحلاف الدولية مثل حلف وارسو (WARSAW PACT) وحلف الناتو (NATO) ، وسنعرض هنا فكرة استخدام حلف الناتو لتلك الطائرات ثم نعرض بعض أنواع هذه الطائرات لتتكون لدينا فكرة عن إمكانات هذا النوع من الطائرات.

(١) مجلة MILITARY TECHNOLOGY عدد مارس ١٩٨٤م صفحة ٢٠.
(٢) كتاب INTELLIGENCE WARFARE للمؤلف الكولونيل وليم كيندي صدر عام ١٩٨٣م صفحة ٩٢.
(٣) مجلة AIR FORCE MAGAZINE الأمريكية عدد يوليو ١٩٨٢م صفحة ٧٨.

٣ ـ طائرات الإنذار المذكر لحلف شمال الأطلسي « الناتو »
NAEW- NATO AIRBORNE EARLY WARNING

طرحت فكرة استخدام حلف الناتو لهذا النوع من الطائرات في ديسمبر عام ١٩٧٨م، ثم تبلورت هذه الفكرة وكون حلف الناتو قيادة لهذه الطائرات في يناير عام ١٩٨٠، بقيادة الميجز جنرال ل. آر بالمرتون الأمريكي(١).

وكانت هناك عدة أسباب دعت الحلف لضم هذا النوع من الطائرات إليه: منها أن الطائرات الروسية المتطورة تستطيع أن تحلق بطيران منخفض جدا دون أن تكتشفها رادارات الحلف قرب الحدود الفاصلة(٢). وعلى سبيل المثال:

١ ـ طائرات باك فير (BACKFIRE) الروسية التي تستطيع أن تطير طيرانا منخفضا من مدينة ايڤور (IVOR) والوصول إلى أهداف في عمق أوروبا الغربية والبحر المتوسط.

٢ ـ طائرة سوخوي ١٩ فنسر (SU-19 FENCER) التي تستطيع أن تطير من ألمانيا الشرقية بطيران منخفض جدا وأن تصل إلى أي من عواصم حلف الناتو في أوروبا الغربية بسهولة محملة بـ ٢٠٠٠ كيلو غرام من المواد المتفجرة.

٣ ـ طائرتا ميج ٢٧ (MIG-27 FLOGGER) وسوخوي ٢٠ (SU-20 FITTER) اللتان تستطيعان التحليق بطيران منخفض جداً وأن تصل بسهولة إلى أي هدف في ألمانيا الغربية وحمولة كل منهما ٤٠٠٠ كيلو غراما من المواد المتفجرة. ولهذه الطائرات القدرة على التحليق المنخفض بسرعة الصوت مستفيدة من العوامل والتأثيرات الأرضية (GROUND CLUTTER) التي تحميها من الكشف بالرادارات الأرضية والجوية، كما أن سرعتها الهائلة بهذا التحليق المنخفض لا يعطي قيادة حلف الناتو الوقت الكافي للتصدي لها.

وكانت التوصيات الرئيسية لحلف الناتو بشأن طائرات الإنذاب المبكر هي :

---

(١) انظر مجلة حلف الناتو عدد خاص يناير ١٩٨٢ NATO'S FIFTEEN NATIONS, SPECIAL ISSUE 1/1982 صفحة ٤٦ مقال الميجر جنرال بالمرتون قائد NAEW

(٢) انظر المصد السابق.

١ ــ شراء ١٨ طائرة من طائرات أواكس أمريكية، نوع (E-3A STANDARD) لتقوم بالتغطية الجوية لدول أوروبا الغربية ويكون مقرها قاعدة (GEILENKIRCHEN) وهي قاعدة العمليات الرئيسية (MOB-MAIN OPERATING BASE) في ألمانيا الغربية، فلو أن ثلاثا من هذه الطائرات قامت بالتحليق في الأجواء الألمانية الغربية فإنها تستطيع في نفس الوقت تغطية الجزء الشرقي من دول أوروبا الغربية. ويكون تسليم الطائرات للعمل في فبراير عام ١٩٨٢م، ويكتمل العدد كله في يونيو ١٩٨٥م. وأن يكون طاقم الطائرات من جميع بلدان حلف الناتو.

٢ ــ شراء ١١ طائرة من طائرات أواكس إنجليزية نوع (NIMROD AEW MK-3) لتغطية بحر الشمال وبحر البلطيق ويكون مقر قيادتها قاعدة وادنكتون (WADINGTON) وهي إحدى قواعد سلاح الطيران الملكي البريطاني في إنجلترا، ويكون تسليم الطائرات للعمل ابتداء من يونيو عام ١٩٨٣م ويكتمل العدد في عام ١٩٨٧م. ويكون جميع طاقمها من سلاح الطيران الملكي البريطاني.

٣ ــ وتقوم جميع هذه الطائرات ببث معلوماتها إلى مركز القيادة العليا للحلف حيث يستفيد منها في عملياته الدفاعية والهجومية التكتيكية والإستراتيجية، كما تساند هذه الطائرات بشكل مباشر مركز عمليات قوات الدفاع الجوي ومركز القوات البحرية لحلف الناتو.

أ ـ طائرة الأواكس الأمريكية AWACS E-3A

١ ــ كلمة أواكس اختصار لكلمات : (AWACS- AIRBORNE WARNING AND CONTROL SYSTEM) أي نظام الإنذار والتحكم الجوي.

٢ ــ في عام ١٩٦٣ بدأ تصميم وتعديل طائرة البوينج ٧٠٧ (BOEING 707) الأمريكية لإعدادها لأن تكون طائرة الأواكس فيما بعد.

٣ ــ تسلمت قوات الطيران الأمريكية أول دفعة من طائرات الأواكس في مارس ١٩٧٧م[١].

(١) مجلة FLIGHT INTERNATIONAL عدد ١٩٨٤/٥/٢٦ صفحة ١٤١٩.

٤ ــ طائرة الأواكس لها طاقم يتكون من :
عدد ٤ طيارين.
عدد ١٣ فردا للانذار والتحكم.

٥ ــ تستطيع طائرة الأواكس أن تبث جميع معلوماتها أوتوماتيكيا للقيادة الأرضية مستخدمة نظام إتصالات يسمى: نظام توزيع المعلومات التكتيكية المشتركة (JTIDS- JOINT TACTICAL INFORMATION DISTRIBUTION SYSTEM) وهو نظام إتصال متطور ذو مجال عريض من ٩٦٠ إلى ١٢١٥ ميغا هرتز أي مجال عرضه ٢٢٥ ميغا هرتز وهو يعمل بطريقة (DIRECT SEQUENCE SPECTRUM SPREADING) وهي طريقة يصعب التشويش عليها وهذا النظام من ابتكار وصناعة شركة هيوز (HUGHES) الأمريكية.

وكذلك تستطيع الطائرة الإتصال المباشر مع الطائرات المقاتلة الصديقة ومع المواقع الأرضية وبطاريات الدفاع الجوي.

وتستطيع طائرة الأواكس أيضاً القيام بمهمة القيادة والسيطرة والإتصالات التكتيكية[١].

٦ ــ بعض طائرات الأواكس وخاصة التي يملكها سلاح الطيران الأمريكي يوجد بها أجهزة تشويش على إتصالات العدو ورااداراته.

كما وأن لها القدرة على التخلص إلكترونيا من التشويش على إتصلاتها بإستخدام نظام الإتصال المتطور (JTIDS) ذي المجال العريض.

أما رادار الكشف والإنذار بطائرة الأواكس فيمكنه التخلص من التشويش الراداري الموجه إليه باستخدام: الصمت الراداري أو بالشعاع الراداري الضيق (عرضه درجة واحدة) ($NARROW\ RADAR\ BEAM\ WIDTH\ 1^{o}$).

٧ ــ القلب النابض لطائرة الأواكس هو رادار الكشف والإنذار (AN/APY-2) الذي يرى مثبتا فوق هيكل الطائرة ويدور بحركة بطيئة (٦ دورات في الدقيقة)، وهو من إنتاج شركة (WESTINGHOUSE) الأمريكية، وله الخواص التالية:

---

(١) مجلة AIR FORCE MAGAZINE الأمريكية صفحة ٧٨. عدد يوليو ١٩٨٢م.

أ ـ يعمل في المجال من ٢٠٠٠ ـ ٤٠٠٠ ميغا هرتز.
ب ـ يعمل باستخدام طريقة (PULSE) أو بطريقة (PULSE DOPPLER).
جـ ـ إذا كانت طائرة الأواكس على ارتفاع ٢٩ ألف قدم يستطيع الرادار كشف الأهداف وهي على بعد ٣٧٠كم(١)، حيث أنه في هذا البعد تكون مدة الإنذار سابقة على إنذار الرادارات الأرضية الكاشفة بثلاثين دقيقة قبل هجوم الطائرات المعادية ذات التحليق المنخفض.
د ـ يكون الكشف والإنذار لطائرة الأواكس الأمريكية فوق الماء واليابسة وليس فوق الماء فقط كما يحدث في طائرة الإنذار المبكر الإنجليزية نمرود (NIMROD MK-3).
هـ ـ ولهذا النوع من الرادار ستة أنظمة منها : كشف الأهداف المنخفضة جداً، والأهداف العالية جداً، ونظام الصمت الراداري (أي بدون إرسال) لمراقبة أي إرسال راداري وتحديد موقعه.
و ـ يستطيع الرادار تحديد موقع أجهزة التشويش الرادارية المعادية.

كما أن طائرة الأواكس الأمريكية مزودة بجهاز كمبيوتر (وشاشات تحكم وهي من انتاج شركتي (IBM) و (HAZELTINE) الأمريكيتين ويقوم جهاز الكمبيوتر هذا بجمع كل المعلومات من أجهزة (IFF) والرادار الإيجابي والرادار السلبي ليكون بالإمكان كشف وتحديد حوالي ٤٠٠ هدف معاد(٢) وتوجيه حوالي ٨٥ طائرة مقاتلة صديقة.

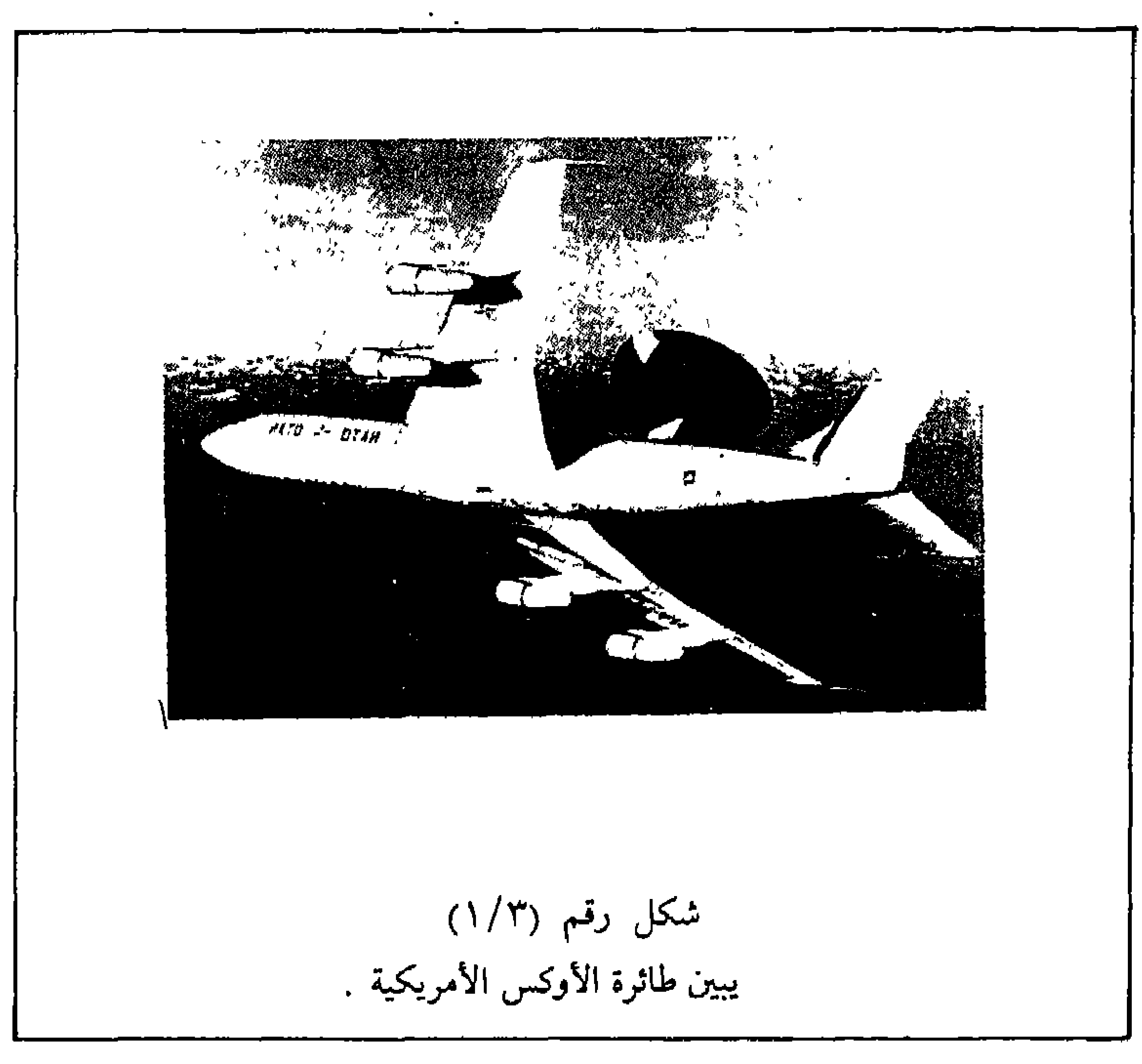
طائرات الأواكس في العالم :

(أ) ـ الولايات المتحدة الأمريكية :

بلغ عدد طائرات الأواكس المملوكة لسلاح الطيران الأمريكي حتى يناير عام ١٩٨٤ (٣١) طائرة، وسيحصل السلاح على ١٨ طائرة أخرى ليصبح المجموع في المستقبل ٤٩ طائرة أواكس(٣).

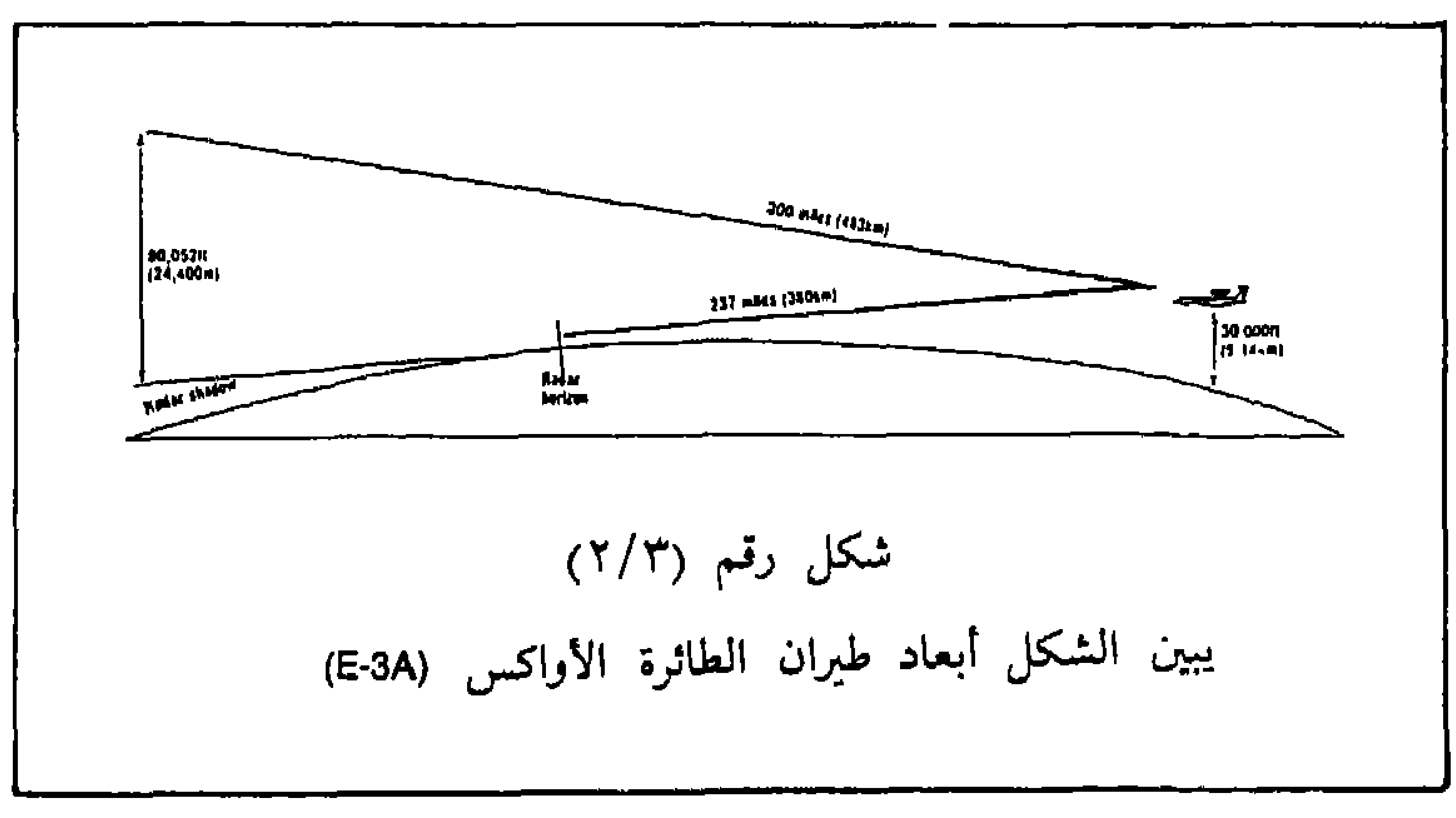
---

(١) كتاب AIRBORNE EARLY WARNING صفحة ١٠٩
(٢) كتاب AIRBORNE EARLY WARNNING صفحة ١١٦.
(٣) مجلة FLIGHT INTERNATIONAL تاريخ ١٩٨٤/٥/٢٦ صفحة ١٤١٩.



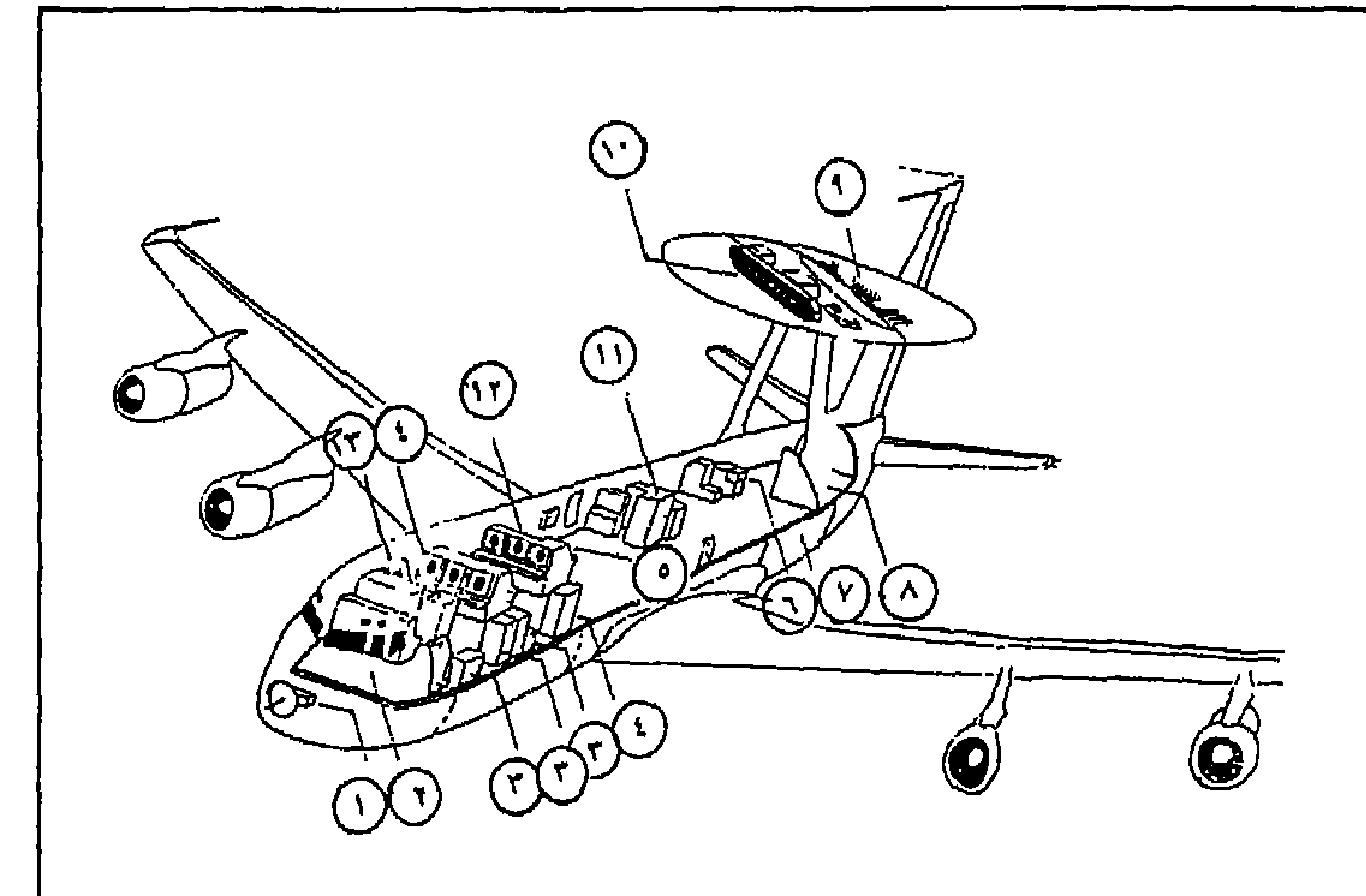
شكل رقم (٣/١)

يبين طائرة الأوكس الأمريكية .



شكل رقم (٣/٢)

يبين الشكل أبعاد طيران الطائرة الأواكس (E-3A)



شكل رقم (٣/٣)

يبين الأجهزة المهمة في طائرة الأواكس (AWACS)

١ ـ رادار الطقس.

٢ ـ الطيار والمساعد والملاح (ومكان آخر احتياط).

٣ ـ أجهزة الإتصالات .

٤ ـ الكمبيوتر.

٥ ـ الضابط المسئول.

٦ ـ أجهزة (I.F.F.) والملاحة.

٧ ـ جهاز إرسال الرادار.

٨ ـ مكان استراحة الطاقم.

٩ ـ هوائي (I.F.F.).

١٠ ـ هوائي الرادار.

١١ ـ جهاز الاستقبال للرادار والكمبيوتر.

١٢ ـ الشاشات المتعددة الأغراض.

١٣ ـ ضابط الكمبيوتر.

(ب) ـ حلف الناتو :

بلغ عدد الطائرات الأواكس المملوكة لحلف الناتو حتى يناير عام ١٩٨٤م (٩) طائرات وسيحصل الحلف على عدد (٩) طائرات أخرى ليصبح المجموع (١٨) طائرة أواكس في يونيو ١٩٨٥[١].

(جـ) ـ المملكة العربية السعودية :

في ديسمبر سنة ١٩٨١ وقعت المملكة العربية السعودية عقدا لشراء (٥) طائرات أواكس أمريكية، يتوقع وصول الدفعة الأولى منها في منتصف ١٩٨٦ وتكتمل في عام ١٩٨٧[٢].

(د) ـ فرنسا :

طلبت فرنسا شراء عدد (٣) طائرات أواكس أمريكية.

ب ـ طائرة عين الصقر الأمريكية GRUMMAN HAWKEYE E-2C

صممت في عام ١٩٦٥م بناء على طلب القوات البحرية الأمريكية لتكون بدلا من طائرة (GRUMMAN E-1B TRACER) القديمة. وهذه الطائرة من إنتاج شركة (GRUMMAN AEROSPACE CORP) الأمريكية. وكان أول طيران تجريبي لها في يناير عام ١٩٧١م.

وتتمتع هذه الطائرة بإمكانية الكشف والانذار المبكر فوق اليابسة والماء. وهي مزودة برادار (AN/APS-125) من إنتاج شركة (GENERAL ELECTRIC) الأمريكية، ومن مميزاته أنه:

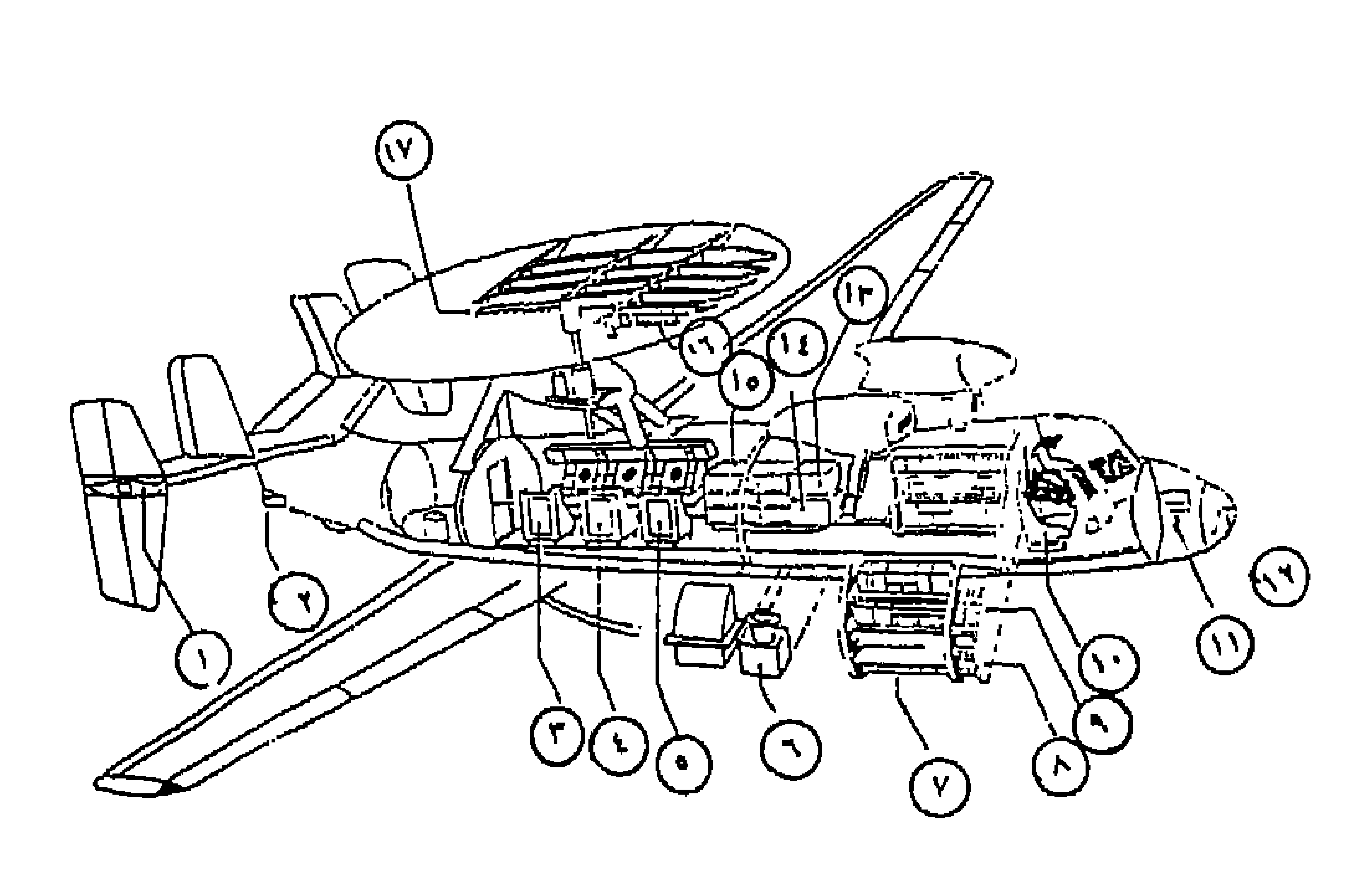
إذا كانت الطائرة على ارتفاع ٣٠ ألف قدم يستطيع الرادار كشف الأهداف حتى ولو كانت على بعد ٤٨٠ كم[٣].

(١) المصدر السابق.
(٢) المصدر السابق.
(٣) كتاب WORLD ELECTRONIC WAREFARE AIRCRAFT صفحة ٦٢.



شكل (٣/٤)

يبين طائرة الانذار المبكر الجوية الأمريكية نوع عين الصقر (HAWKEYE E-2C) .



شكل رقم (٣/٥)

يبين الشكل الأجهزة المهمة لطائرة عين الصقر (E-2C).

١ ـ هوائي مراقبة الموجات.
٢ ـ هوائيات مراقبة الموجات.
٣ ـ ضابط السيطرة الجوية.
٤ ـ ضابط معلومات المعركة.
٥ ـ ضابط الرادار.
٦ ـ جهاز موجه المدى.
٧ ـ الأجهزة الإلكترونية.
٨ ـ الأجهزة الملاحية.
٩ ـ أجهزة التشفير.
١٠ ـ الطيار ومساعده.
١١ ـ الأجهزة الملاحية.
١٢ ـ هوائيات مراقبة الموجات.
١٣ ـ كمبيوتر الرادار.
١٤ ـ كمبيوتر جهاز (I.F.F.).
١٥ ـ الكمبيوتر.
١٦ ـ هوائي جهاز (I.F.F.).
١٧ ـ هوائي الرادار.

كما أن طائرة عين الصقر (E-2C) مزودة بجهاز مراقبة (AN/ALR-59) (رادار سلبي PASSIVE RADAR) وهو من إنتاج شركة ليتون (LITTON) الأمريكية، ويستطيع الكشف والإنذار عن أي جهاز إرسال أو جهاز تشويش على بعد ٣٧٠ كم(١).

أما طاقم الطائرة فيتكون من عدد ٥ أشخاص للقيام بعدة مهام، منها:
مراقبة جميع الطائرات المحلقة في مجال الرادار.
وتوجيه طائرات خفر السواحل والهليوكبتر.
وكما توجه الطائرات الإعتراضية في المعركة، وتقوم أيضا بالمراقبة الدقيقة لجميع الأهداف التي تحلق فوق اليابسة والماء حتى ولو كانت على هيئة صاروخ متوسط الحجم على بعد ١٨٥كم.

كما أن لطائرة عين الصقر جهاز (IFF (IDENTIFICATION FRIEND OR FOE لتمييز الأهداف الصديقة عن الأهداف المعادية.

وجميع معلومات أجهزة (IFF) والرادار الإيجابي (AN/APS-125) والرادار السلبي (AN/ALR 59) تصب في جهاز (CENTRAL PROCESSOR OL-77/ASQ) وهو من إنتاج شركة (LITTON) الأمركية فيكون بالإمكان كشف وتحديد حوالي ٢٥٠ هدفاً معادياً وتوجيه ٣٠ طائرة مقاتلة صديقة.

والجدير بالذكر أن اسرائيل استطاعت اجراء بعض التعديلات على طائراتها الأربع (E-2C) فجعلت كل طائرة منها تستطيع توجيه ١٥٥ مقاتلة صديقة بدلاً من ٣٠ طائرة(٢).

كما قام الأمريكيون عام ١٩٨٢ بإضافة جهاز ثان إلى جهاز .CENT. PROC (OL-77/ASQ.) وهو جهاز كمبيوتر (L/304) من إنتاج شركة (LITTON) الأمريكية، وبذلك يكون بالإمكان كشف وتحديد حوالي ٦٠٠ هدف معادي وتوجيه حوالي ٤٠ طائرة مقاتلة صديقة.(٣).

---

(١) المصدر السابق.
(٢) مجلة AVIATION WEEK & SPACE TECHNOLOGY عدد ١٩٨٢/٧/٥م صفحة ١٦.
(٣) كتاب AIRBORNE AERLY WARNNING صفحة ٩٨.

٧ ـ طائرات E-2C في العالم :

ـ الولايات المتحدة الأمريكية: مجموع طلباتها ١٠٢ طائرة[١].
ـ جمهوية مصر العربية سيبلغ عدد الطائرات المملوكة لجمهورية مصر العربية خلال عام ١٩٨٥ ٤ طائرات[٢].
ـ إسرائيل : طلبت إسرائيل ٤ طائرات[٣] في عام ١٩٧٦ وحصلت عليها في عام ١٩٧٨، واستخدمتها في حرب لبنان في يونيو عام ١٩٨٢م
ـ اليابان: طلبت اليابان ٨ طائرات[٤].
ـ سنغافورة: طلبت سنغافورة ٤ طائرات[٥]

كما أن هناك دولا قدمت طلبا لشراء هذا النوع من الطائرات، وهي : استراليا، كوريا الجنوبية، اليونان، فرنسا، سويسرا.

(١) و(٢) و(٣) و(٤) و(٥) مجلة FLIGHT INTERNATIONAL تاريخ ١٩٨٤/٥/٢٦م صفحة ١٤٢٠.

٤ ـ طائرة الأواكس الروسية MOSS

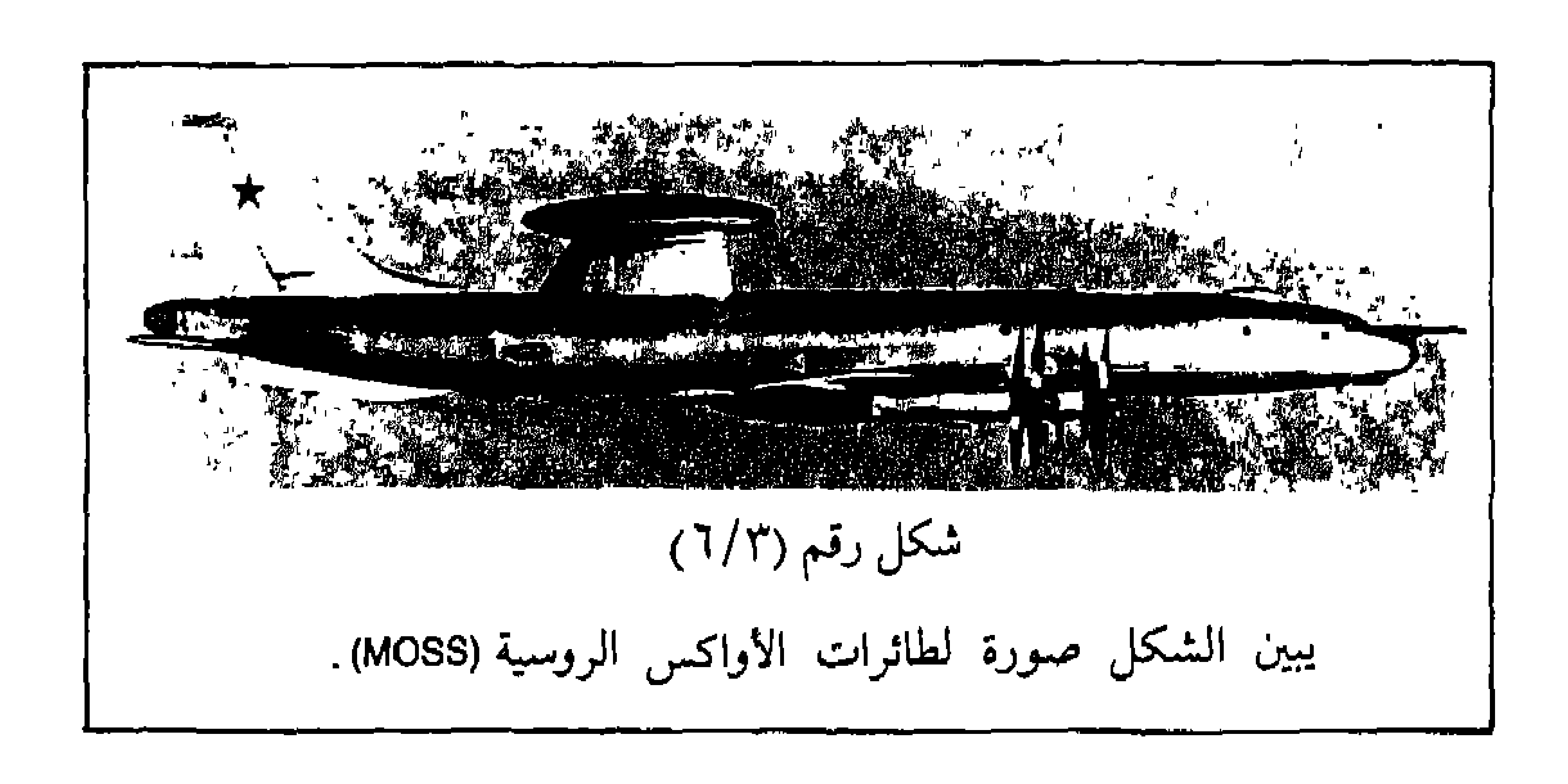
أطلق اسم (MOSS) على طائرة الأواكس الروسية من قبل حلف الناتو، وفي عام ١٩٦٠ بدأ تصميم وتعديل طائرة توبوليف ١٢٦ (TUPOLEV TU-126) لإعدادها لتكون طائرة أواكس فيما بعد وكان أول طيران تجريبي لها في عام ١٩٦٢م.

وهي تقارن بطائرة الأواكس الأمريكية من حيث الانذار والتوجيه، كما أن لها رادار يستطيع كشف الأهداف على بعد ٣٧٠ كم وهي على ارتفاع حوالي ٢٠ ألف قدم.

ومعظم طائرات (MOSS) مزودة بأجهزة تشويش على الإتصالات والرادارات.

وقد بلغ عدد طائرات الأواكس (MOSS) المملوكة لسلاح الطيران الروسي في عام ١٩٧٠م (٢٠) طائرة.

ويقال أن الهند استخدمتها في حربها ضد باكستان عام ١٩٧١م.

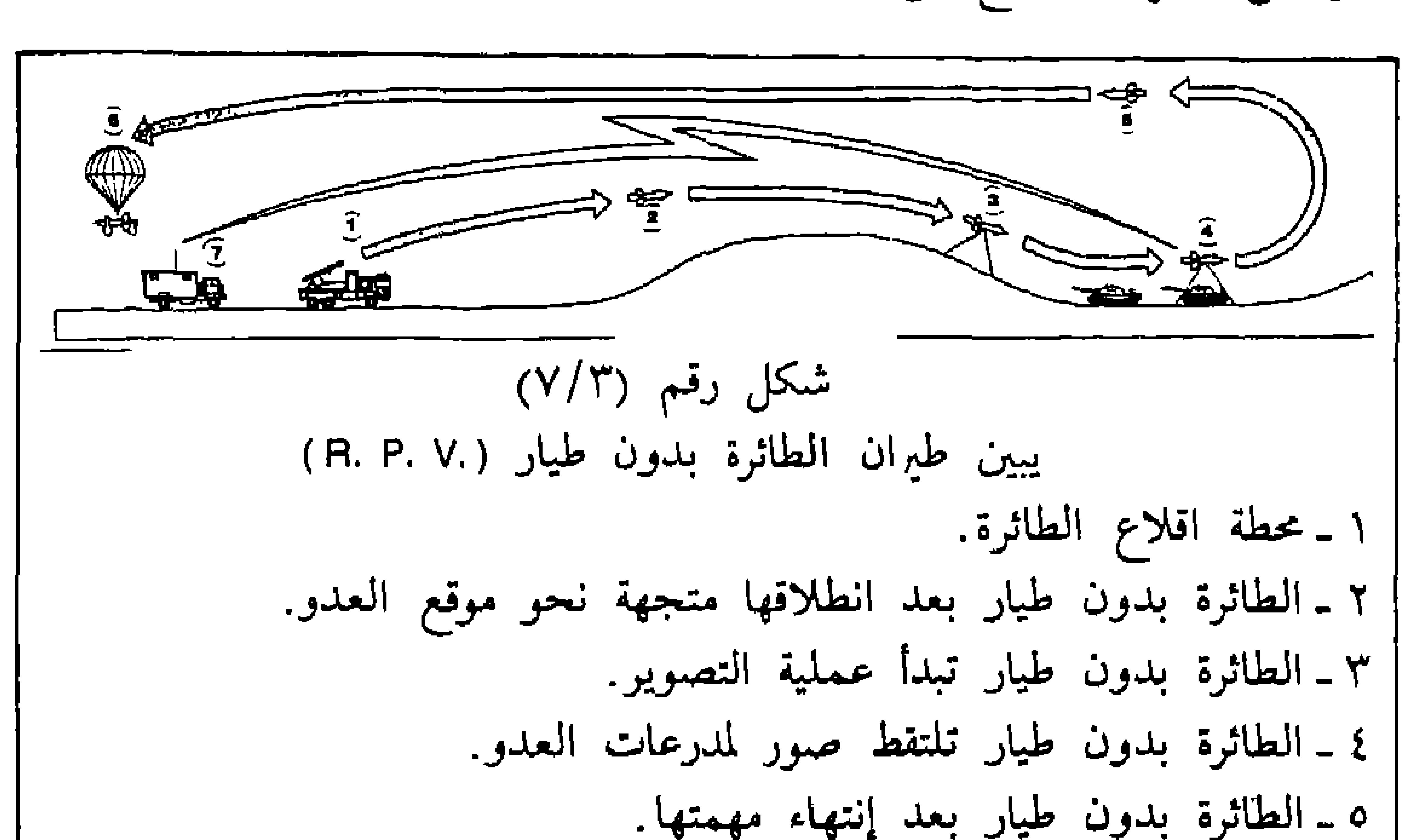


شكل رقم (٦/٣)

يبين الشكل صورة لطائرات الأواكس الروسية (MOSS).

٥ ـ الطائرات بدون طيار RPV, DRONE

الطائرة بدون طيار، هي عادة طائرة صغيرة الحجم بالنسبة للطائرات الحربية ولها محرك مروحي تطير باستخدام طريقة التحكم عن بعد (REMOTE CONTROLLING) بواسطة موجات لاسلكية، وتقوم بأعمال مختلفة. انظر شكل رقم (٧/٣) وهي إما أن تطلق من طائرة أو تقلع من سفينة أو محطة أرضية.



شكل رقم (٧/٣)

يبين طيران الطائرة بدون طيار (.R. P. V)

١ ـ محطة اقلاع الطائرة.
٢ ـ الطائرة بدون طيار بعد انطلاقها متجهة نحو موقع العدو.
٣ ـ الطائرة بدون طيار تبدأ عملية التصوير.
٤ ـ الطائرة بدون طيار تلتقط صور لمدرعات العدو.
٥ ـ الطائرة بدون طيار بعد إنتهاء مهمتها.
٦ ـ الطائرة بدون طيار تستخدم المظلة للهبوط.
٧ ـ مركز التحكم عن بعد للطائرة.

ولكي تؤدي الطائرة مهمتها فإنها تحتاج إلى:

أ ــ مركز تحكم ومراقبة.
ب ــ قاعدة أو مدرج إقلاع.
جـ ــ شبكة في مكان الاقلاع لصيد الطائرة عند رجوعها من مهمتها، أو تستخدم الطائرة المظلة الجوية (PARACHUT) للهبوط.

وهناك نوع من تلك الطائرات تطير مرة واحدة لتؤدي مهمة ما. ثم تسقط فوق مواقع العدو لتدمرها.

ولهذه الطائرة مسميان:

الأول: (DRONE)

والثاني: (R.P.V - REMOTELY PILOTED VEHICLE)

والفرق بين النوعين أن الأولى عادة تكون مبرمجة لتؤدي مهمة محددة والثانية يتم التحكم في طيرانها كليا وعن بعد بطريقة (REMOTE CONTROLING) بواسطة إرسال موجات لاسلكية لتأدية مهمات مختلفة.

نبذة تاريخية عن الطائرة بدون طيار:[1]

أ ـ حلقت أول طائرة بدون طيار في عام ١٩٣٤م وكان تسمى آنذاك « ملكة النحل » (QUEEN BEE) وكانت مستخدمة من قبل القوات البحرية الملكية البريطانية.

ب ـ استعلمت تلك الطائرة للتمويه والخداع، إذ استخدمت كطعم للرادارات الأرضية لتظهر على شاشاتها وكأنها كبيرة الحجم وذلك في عام ١٩٤٤م.

جـ ـ كانت أول طائرة (R P V) استطلاعية متطورة من إنتاج شركة (CANADA AIR).

د ـ ومن أكثر الطائرات التي تطير بدون طيار وتمت تجربتها في الحروب وأثبتت كفاءتها، الطائرات الإسرائيلية الصنع، التي استخدمت في حرب لبنان عام ١٩٨٢.

كما تذكر التقارير أن من الأسباب الرئيسية التي أدت إلى بطء تطور صناعة الطائرات بدون طيار وخاصة (R. P. V.) هي:

أن معظم استخدامات هذه الطائرات كانت فقط كطعم للرادارات الأرضية (DECOY,) أو (TARGET).

ويطلق على الطائرة بدون طيار المنطلقة من الطائرات اسم الطعم (DECOY) والطائرة المنطلقة من الأرض اسم الهدف (TARGET) وهي عادة من طائرات (DRONE) وتستطيع هذه الطائرة حمل معدات مختلفة لتأدية مهام عديدة منها:

أ ـ كاميرات تلفزيونية.

ب ـ كاميرات بانوراما.

---

(١) انظر مجلة MILITARY TECHNOLOGY عدد أكتوبر عام ١٩٨٣م. ص١٤.

جـ ـ جهاز ليزر لتحديد الأهداف وإرشاد الصواريخ إليها. ويطلق عليه اسم (LASER DESIGNATOR).

د ـ أجهزة إلكترونية مساندة (ESM EQUIPMENTS).

هـ ـ أجهزة إلكترونية مضادة (ECM EQUIPMENTS).

و ـ أجهزة أشعة تحت الحمراء للكشف عن الأهداف الليلية (INFRA RED SENSORS)

ز ـ معدات لقذف ما يسمى « بأجهزة التشويش المقذوفة » (PASSIVE ECM CARTRIDGES) مثل: النصلات (CHAFF) ، أجهزة التشويش (EXPENDABLES JAMMERS).

ح ـ أجهزة اتصالات لاسلكية .

ويجب أن تحدد مهمة هذه الطائرة عند صناعتها، فإما أن تكون :

ذات هيكل وطلاء يجعلها تعكس أكبر كمية من أشعة الرادار، لتظهر على شاشته وكأنها هدف كبير الحجم. أو أن تكون على العكس أي ذات هيكل وطلاء يجعلها تعكس أقل كمية من أشعة الرادار لتظهر على شاشته وكأنها نقطة متناهية الصغر. وذلك لتؤدي مهمتها بدون اعتراض من قبل العدو.

ومما تقدم نستطيع حصر مهمات الطائرة بدون طيار في الآتي :

أولا : تستعمل كهدف كبير «طعم» للرادارات الأرضية.

ثانيا : للاستطلاع الجوي.

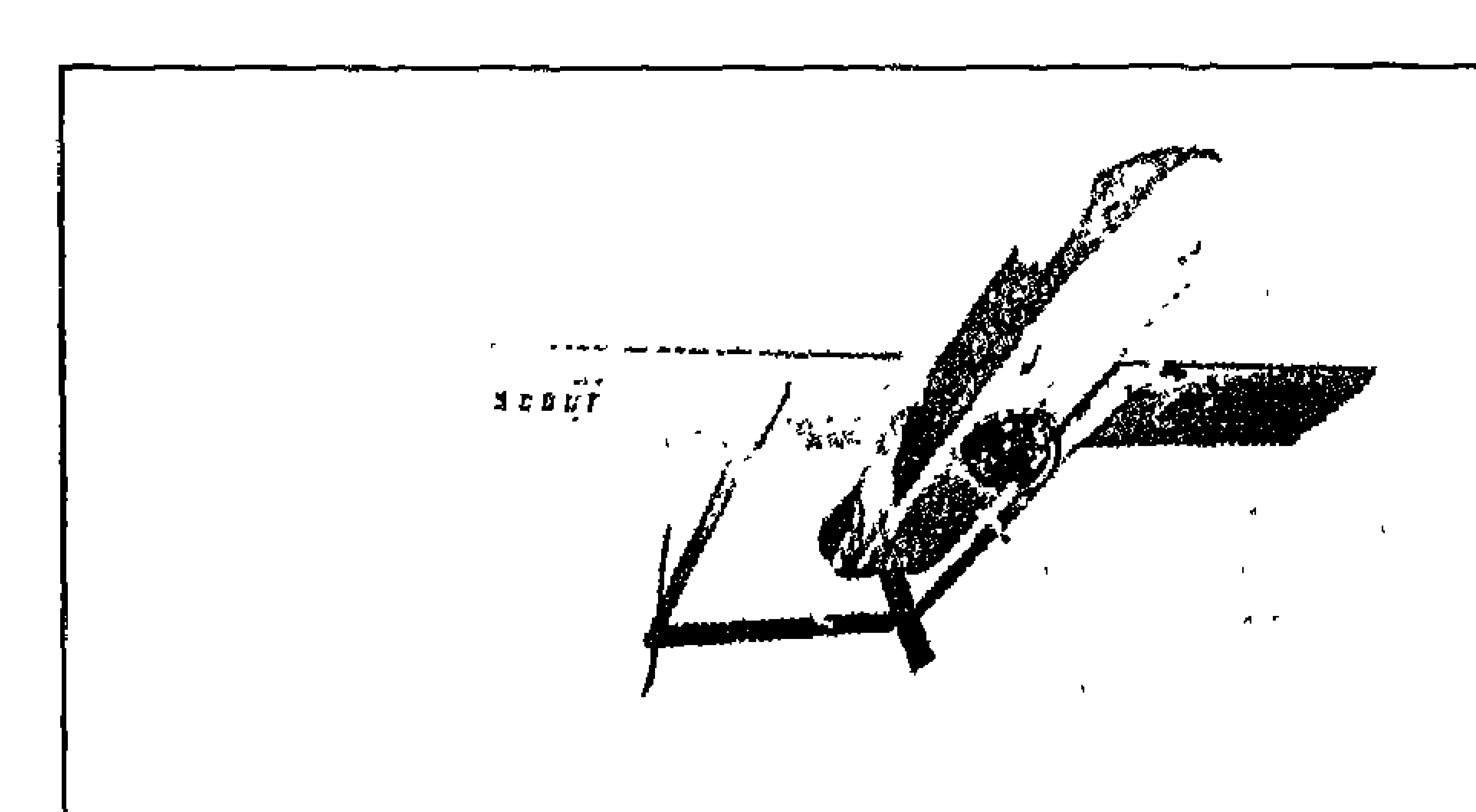
ثالثا : للكشف عن الأهداف الأرضية والبحرية.

رابعا : لاستخدامات أجهزة الإجراءات الإلكترونية المساندة (ESM)، والإجراءات الإلكترونية المضادة (ECM).

وأخيرا كجهاز لتقوية الإتصالات عبر الأفق (RADIO REPEATER) وثمة مواصفات تميز كل نوع من تلك الأنواع وتختلف باختلاف المهمة المصممة لها كل طائرة، وسنذكر هنا مثالاً لأحد أنواع هذه الطائرات :

طائرة سكوت SCOUT R. P. V. :

وطائرة (SCOUT)[1] من إنتاج شركة صناعة الطائرات الإسرائيلية . I.A.I.- ISREAL AIRCRAFT INDUSTRIES) وهي طائرة صغيرة الحجم رخيصة الثمن (حوالي ١٥٠ ألف دولار). تستخدم للإستطلاع الجوي ونقل المعلومات والصور فورا من مواقع العدو إلى مركز القيادة.



شكل رقم (٣/٨)

يبين الشكل صورة للطائرة بدون طيار نوع (SCOUT) الإسرائيلية .

توصي الشركة بأن تتكون محطة الطائرة من:

أ ــ عدد ٦ إلى ٨ طائرات (R. P. V.).

ب ــ عد ١ مركز قيادة وتحكم للطائرة.

جـ ــ عدد ١ منصة أو مدرج إقلاع.

د ــ عدد ١ شبكة لصيد الطائرة عند الهبوط بعد تأدية المهمة.

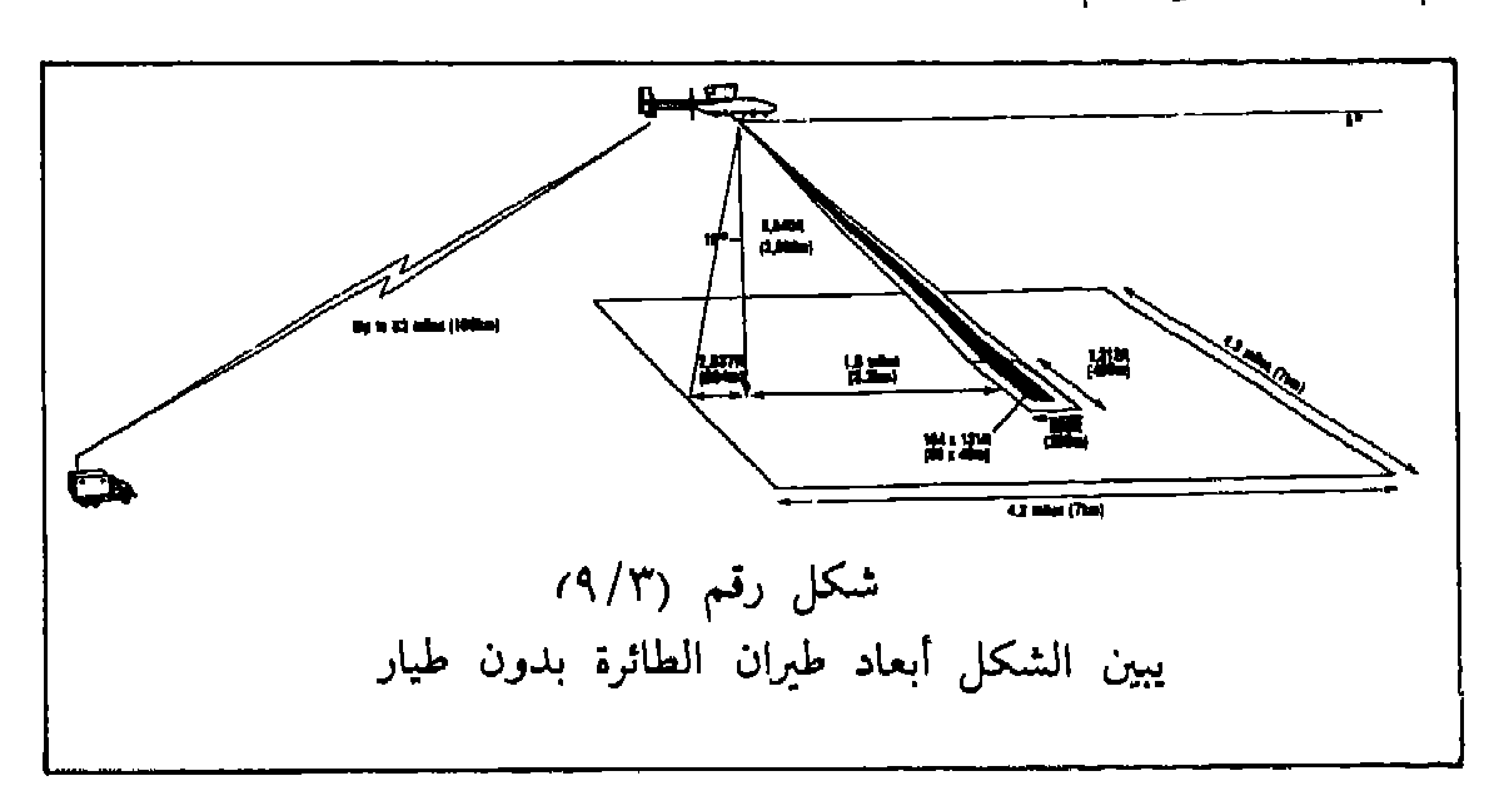
مواصفات طائرة SCOUTالإسرائيلية:

أ ــ الطول ٣,٦٨ مــتر.

ب ــ عرض الجناحين : ٣,٦٠ متر.

(١) مجلة MILITARY TECHNOLOGY صدرت في يونيو ١٩٨٣م صفحة ٤٦.

جـ ـ ارتفاعها عن الأرض ٩٤ سم.
د ـ أكبر حمولة تستطيع حملها ١١٨ كيلوغراما،
هـ ـ المحرك مروحي.
و ـ أقصى سرعة لها ١٠٢ كم / ساعة.
ز ـ أقصى مدة طيران متواصلة حوالي ٤ ساعات.
ع ـ أقصى إرتفاع تصل إليه الطائرة حوالي ١١ ألف قدم عن سطح الأرض.
غ ـ لكي تؤدي الطائرة مهمتها يجب ألا تزيد المسافة بينها وبين مركز القيادة عن ١٠٠ كم. انظر شكل رقم (٣/٩).



شكل رقم (٣/٩)
يبين الشكل أبعاد طيران الطائرة بدون طيار

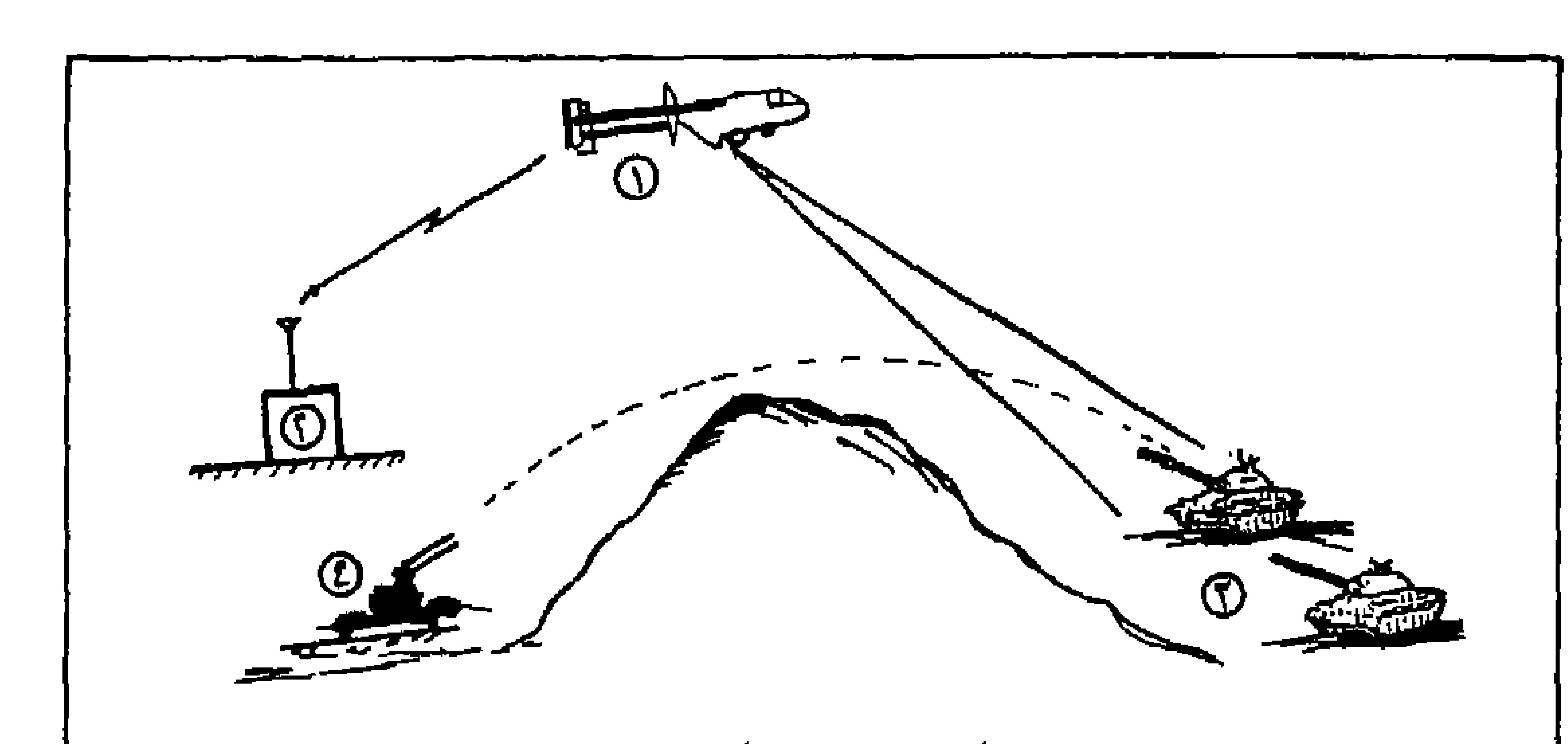
وتستطيع طائرة (SCOUT) حمل الآتي :
أ ـ كاميرا تلفزيونية لتصوير المواقع التي تحلق فوقها الطائرة ونقل المعلومات فورا بإرسالها بموجات لاسلكية إلى مركز القيادة أو أية غرفة عمليات.
ب ـ كاميرا بانورما.
جـ ـ أجهزة (ESM, ECM).

أما بالنسبة للتحكم في طائرة (SCOUT) وهي محلقة فيكون يدويا (MANUALLY) أو أوتوماتيكيا (AUTOMATIC) باستخدام (AUTO-PIOLT) أوبجهاز مبرمج.

وتستخدم تلك الطائرات في المهام الآتية:
أ ـ في المراقبة والإستطلاع الجوي والتشويش.

ب ـ في مراقبة مواقع العدو وإرسال المعلومات لأية جهة ولأي عدد من المراكز.

جـ ـ تستخدم في مساعدة المدافع الأرضية من حيث نقل إحداثيات الأهداف التي يراد تدميرها إلى قيادة المدفعية حتى ولو كان الهدف وراء الأفق أو وراء تلال أو جبال، كما أنها تعطي معلومات لمركز القيادة بهدف تصحيح الرمي إذا لم تكن الإصابة مباشرة. انظر شكل قم (٣/١٠).



شكل رقم (٣/١٠)

١ ـ طائرة بدون طيار تستخدم لتصوير موقع العدو.
٢ ـ محطة تحكم.
٣ ـ موقع العدو.
٤ ـ المدفعية.

يبين الشكل كيفية استخدام الطائرة بدون طيار لتصوير موقع العدو، وإرسال الصور لاسلكيا إلى مركز التحكم لإعطاء المعلومات للمدفعية لقصف ذلك الموقع.

د ـ أن تكون محملة بقنابل شديدة الإنفجار لتدمير مواقع العدو.

هـ ـ تستخدم كذلك للطيران في عمق أرض العدو وتسجل جميع المعلومات بدون إرسالها « صمت الإتصال » وعند هبوطها يتم الحصول على المعلومات المختزنة بها.

وقد استخدمت طائرة (SCOUT) الإسرائيلية في حرب لبنان عام ١٩٨٢ كالآتي:

أ ـ استعملت لمراقبة القواعد الجوية السورية ونقل معلومات عن عدد هبوط وإقلاع

الطائرات السورية فوراً إلى إسرائيل.

ب ـ استعملت كطعم للرادارات السورية في وادي البقاع لكي يشغل السوريون رادار موجه الصواريخ (FIRE CONTROL RADAR) التابع لصواريخ سام ـ ٦ ومن ثم يتم رصد موجات وذبذبات الرادار للتشويش عليه، وكذلك لتوجيه الصواريخ المضادة للرادارات الأرضية ضد رادارات سام ـ ٦.

جـ ـ استعملت كذلك لتوجيه أشعة الليزر على المواقع السورية لكي ترمي الطائرات الإسرائيلية المسلحة التي توجه بأشعة الليزر قذائفها لتدمير تلك المواقع.

د ـ استعملت للتصوير التلفزيوني للمواقع السورية وكانت للكاميرات ذات قابلية للتقريب (ZOOMING).

مما تقدم نستطيع حصر المحاسن والمساوىء للطائرات بدون طيار فيما يلي:

أولاً : المحاسن :

١ ـ رخيصة الثمن.
٢ ـ ليس هناك خوف على طيار، إذ تستطيع الدخول في عمق أرض العدو.
٣ ـ صغيرة الحجم.
٤ ـ محطة هذه الطائرة سهلة التنقل.
٥ ـ تحتاج إلى وقود قليل وتدريب بسيط.
٦ ـ يسبب سقوطها في الأراضي الصديقة ـ ضررا بسيطاً.
٧ ـ سهولة تشكيلها من حيث الحجم والشكل، إذ ليست مثل الطائرة العادية مقيدة بحجم وراحة الطيار.
٨ ـ يمكن استعمالها في أي وقت وبأكبر كمية من ساعات الطيران بتكاليف تصليح وصيانة قليلة جدا مقارنة بالطائرات الحربية الأخرى.

ثانيا : المساوىء :

١ ـ محدودة الاستعمال أي ذات مهام محدودة ومدى محدود.
٢ ـ مركز التحكم باهظ التكاليف.
٣ ـ احتمال التشويش على موجات التحكم الكهرومغناطيسية، أو التشويش على معلوماتها التي تبثها إلى مركز قيادتها.

الباب الرابع

تطبيقات أسس الحرب الالكترونية في الحروب السابقة

سنستعرض هنا بعض تطبيقات وعمليات أسس الحرب الإلكترونية التي حدثت في الحروب السابقة وهي مما تناقلته وسائل الإعلام من صحف ومجلات وكتب وما نشرته وكالات الأنباء والتقارير الأجنبية المتخصصة وسوف نرى أن هذه التطبيقات قد شملت جميع أسس الحرب الإلكترونية من إستخبارات الإشارة (SIGINT) والإجراءات الإلكترونية المساندة (ESM) والإجراءات الإلكترونية المضادة (ECM) والمضادات الإلكترونية للإجراءات المضادة (ECCM).

في الحرب العالمية الثانية استخدم الألمان ما يسمى بتقاطع إرساليات الراديو (BEAM-INTERSECTION) لتوجيه الطائرات الألمانية القاذفة لقصف المدن الإنجليزية وكانت هذه الطريقة حديثة آنذاك ويسمى هذا النظام بـ(LORENZ)[1] وكانت نتائجها دقيقة إلى حد ما، وبعد فترة وعندما عرف الإنجليز هذه الفكرة عملوا على وضع جهاز إرسال من نفس الموجة ولكن في موقع يترتب عليه أن يكون الـ (INTERSECTION) أو تقاطع الإرسال الألماني منحرفا بدرجات بسيطة تجعل القاذفات الألمانية تقصف مناطق بعيدة نسبيا عن أهدافها الأساسية، ولما كان هذا القصف عادة يتم في الليل فقد نجحت هذه الخدعة نجاحا كبيراً.

في الحرب العالمية الثانية كان الألمان قد وضعوا رادارات إنذار مبكر ومدافع أرض جو على طول الساحل الغربي الفرنسي لحمايته من الهجوم عليه، فلما أراد الحلفاء قصف هذه الرادارات والمدافع تمهيدا لغزو الساحل المذكور أقلعت طائرات نقل كبيرة تحمل أطنانا من النوافذ أو النصلات (CHAFF) تلقيها في الجو موازية للساحل الفرنسي لتصنع ممرا (CORRIDOR) تطير فيه الطائرات القاذفة التابعة للحلفاء وبسرعة تنفذ هذه القاذفات لتقصف المواقع الألمانية وفعلا نفذ الحلفاء عمليتهم، وحققت نجاحا كبيراً.

---

(١) كتاب حرب الإستخبارات INTELLIGENCE WARFARE ص ٧٩.

في عام ١٩٥٢ إكتشفت السفارة الأمريكية بموسكو وجود جهاز تنصت صغير موضوع على شعار أمريكا في غرفة السفير، واتهمت السوفيت بوضعه وعرضته على الأمم المتحدة[١].

كما سلط الروس أشعة ميكروويف على نافذة مكتب السفير الأمريكي في سفارته بموسكو حتى إذا جرى حديث في غرفة السفير اهتز الزجاج فيؤثر ذلك على أشعة الميكروويف، وبتحليل (DOPPLER SHIFTING) يستطيعون معرفة ما يدور من حديث داخل الغرفة.

عندما بنيت السفارة الأمريكية في موسكو وضع السوفييت جهاز تنصت داخل حائط غرفة السفير للتنصت على ما يجري داخل الغرفة، ويغذي هذا الجهاز بتسليط أشعة مايكروويف عن بعد على جهاز التنصت لإعطائه القدرة الكهربائية على العمل، حتى أن السفارة الأمريكية عندما أرادت بناء سفارة جديدة أحضرت كل ماتحتاجه من مواد البناء والأثاث وغيرها من أمريكا.

إستخدم الأمريكان عام ١٩٦٢ طائرة الإستطلاع (U2) لتصوير أول شحنة صواريخ نووية سوفيتية وصلت إلى كوبا وأثيرت بعدها ضجة كبيرة أوشكت على نشوب حرب نووية.

تم القبض على الجاسوس الشهير كوهين في سوريا في منتصف الستينات حيث إكتشف السوريون أمره بتنصتهم على جهازه المرسل عندما كان يرسل معلوماته إلى إسرائيل وهذا شبيه بما حدث عندما ألقي القبض في السبعينات على مساعد المستشار الألماني الغربي فيلي برانت وهو يتجسس لحساب السوفيت ورغم أن المستشار فيلي برانت كان محبوبا في ألمانيا الغربية إلا أن تلك الفضيحة أجبرته على الاستقالة من منصبه.

في حرب ١٩٦٧ قبل هجوم إسرائيل على سيناء بفترة وجيزة قامت بعمل تشويش

---

(١) كتـاب حـرب الإستخبارات INTELLIGENCE WARFARE ص ٧٢.

عريض المجال (تشويش وابل) على جميع أجهزة الإتصالات المصرية في سيناء مما ساعد على سهولة احتلالها.

عمدت أمريكا في حرب ١٩٦٧ إلى إرسال بعض طياريها العسكريين وطائرات فانتوم بها أجهزة تصوير متطورة تصور جميع التحركات العربية وخاصة الليلية باستخدام آلات تصوير حساسة للأشعة تحت الحمراء (INFRARED SENSORS) وإعلام الجيش الإسرائيلي بذلك لقصفها وكان على هذه الطائرات شعار نجمة داود للتمويه.

في حرب ١٩٦٧ م بعد أن غنمت إسرائيل عدد من بطاريات سام ٢ من سيناء ، عمل الإسرائيليون والخبراء الأمريكيون على معرفة خواص وموجات تلك الصواريخ وبذلك استطاع الأمريكيون التشويش الوابل على جميع صواريخ سام ٢ في فيتنام عندما أرادوا قصف هانوي وهايبونغ بطائرات (B-52) وكانت النتائج إيجابية للغاية حيث زادت الخسائر الفيتنامية، وقلت الخسائر الأمريكية بشكل ملحوظ.

في عام ١٩٦٨ عندما أراد السوفييت غزو تشيكوسلوفاكيا أطلقوا أطناناً من النصلات (CHAFF)في الجو على الحدود بين تشيكوسلوفاكيا والدول الغربية وعملوا تشويشا على جميع الإتصالات لتعيق جميع أجهزة الدول الغربية حتى لا تعلم بما يجري ليتم الغزو كاملا دون تدخل أو احتجاج . وفعلا تم الهجوم بهدوء وبنجاح ولم تعلم الدول الغربية عنه شيئاً إلا نهاراً ، بعد فوات الأوان .

وعزا الخبراء هذا إلى أن السوفيت عملوا (ELECTRONIC BLANKET) وحجبوا تشيكوسلوفاكيا تماما عن العالم الخارجي.

قبل هجوم السوفيت على تشيكوسلوفاكيا عام ١٩٦٨ وقبل هجوم الأرجنتين على فوكلاند عام ١٩٨٢ ، تم القبض على جميع هواة الاسلكي ومصادرة أجهزتهم ثم فرضت مراقبة مكثفة على أي إرسال لبضعة أسابيع حتى تستطيع الدولة المهاجمة تنفيذ الهجوم والإحتلال قبل أن ينتقل الخبر إلى باقي دول العالم.

في الحرب الهندية الباكستانية عام ١٩٧١ ألقى القبض في كلتا الدولتين على

أشخاص معهم أجهزة إرسال صغيرة يوجدون قرب القواعد الجوية لإعلام دولهم بعدد الطائرات المقلعة والهابطة وأنواعها وتسليحها.

في حرب ڤيتنام إستخدم الأمريكان للكشف عن الثوار الڤيتناميين في الغابات الكثيفة أجهزة إلكترونية دقيقة تلقى في الغابات لإكتشاف وإرسال المعلومات إلى القيادة وهم يحصلون على هذه المعلومات من الإهتزازات الأرضية التي تبين سير الثوار على الأرض كما أن بعض الأجهزة كانت تستخدم لإكتشاف الإنسان من خلال التقاط إفرازاته الجسمية.

إستطاعت إسرائيل في أوائل السبعينات وضع أجهزة تنصت على أعمدة التلفونات الأردنية المتصلة بقاعدة عسكرية وإكتشفت هذه الأجهزة بعد فترة طويلة.

في حرب ١٩٧٣ لاحظت القوات العربية في الجبهة السورية سهولة وقوع أسرى إسرائيليين في أيديهم وكأنهم يتطوعون للأسر، ولما كان هذا الشيء مثير للريبة، أجريت بعض التحقيقات والتحليلات، إتضح منها أن هؤلاء أشخاص مدربون للتغلغل في الأراضي السورية لوضع أجهزة استقبال وإرسال للتنصت على القوات العربية ومعرفة محادثاتهم وتحركاتهم أولا بأول.

في حرب ١٩٧٣ استطاعت سورية عمل تشويش وابل على جميع الذبذبات في مجال موجات الدبابات الإسرائيلية ونجحت بذلك نجاحا تاما ولكن أدى هذا إلى التشويش على الأجهزة السورية أيضاً .

إستطاع الإسرائيليون في حرب ١٩٧٣ باستخدام أجهزة التنصت والمراقبة تتبع نتائج قصف طائراتهم للمواقع العربية، إذ أنه في أثناء القصف وبعده يستمعون إلى النتائج عبر أجهزة الراديو بعد أن ترد من المواقع العربية المقصوفة إلى مراكز القيادة العربية ـ وبتحليلها يرسلون تلك المعلومات والتصحيحات إلى الطائرات القاذفة الإسرائيلية لكي تقصف المواقع العربية التي لم تدمر بالكامل.

في حرب ١٩٧٣ م كانت جمهورية مصر العربية تستخدم ــــ ضمن قواتها ـ المدفع الرشاش (SHILKA) أرض جو ، وهو روسي الصنع ، فاستطاعت إسرائيل خداعه بطريقة «سرقة بوابة المجال» (RANGE GATE STEELING) ودمرت منه عدداً كبيراً، ولكن ما لبثت

مصر أن عرفت السر في ذلك ، فاستخدمت القوات المصرية المدافع بالتحكم بالعين المجردة ، وأمكنها إسقاط عدد من الطائرات الإسرائيلية بتضاد التشويش .

في حرب ١٩٧٣ إلقي القبض على عدد من رعاة الأغنام في سوريا ومعهم أجهزة إرسال صغيرة (WALKY TALKY) يخاطبون الطيارين الإسرائيليين ويخبرونهم عن تحركات الجيوش العربية في تلك المنطقة لقصفها.

علمت أمريكا بعزم إسرائيل إستخدام صواريخها النووية في حرب ١٩٧٣ بعد المأزق الكبير غير المتوقع الذي وقعت فيه إسرائيل، فأقلعت طائرة إستطلاع أمريكية نوع (BLACK BIRD-SR71) من قاعدة في جورجيا وتزودت بالوقود جوا فوق إسبانيا لتصوير تلك الصواريخ وخط التماس بين الجيوش العربية والإسرائيلية[١].

ولما عادت الطائرة في نفس اليوم إلى القاعدة، أعطيت إسرائيل صورة لثغرة الدفرسوار كي تستعملها بدل الصواريخ النووية.

وضعت ليبيا في أوائل السبعينات ميكروفونات ضخمة على الحدود بينها وبين جمهورية مصر العربية لتتنصت على كل التحركات العسكرية المصرية قرب الحدود .

في ١٩٨١/٥/٧ إستطاع الإسرائيليون قصف المفاعل النووي العراقي وقد استخدموا التشويش الوابل على جميع موجات الإتصالات والرادارات في تلك المنطقة وكذلك على مسار طائرات القصف (F-15, F-16) التي إتخذت مساراتها عبر بعض الدول المجاورة، وقد استغرق تدريب الطيارين عدة شهور قبل تنفيذ عملية القصف.

استخدم الإسرائيليون في أوائل الثمانينات الطائرات بدون طيار (DRONES, PRV) لمراقبة الرادارات السورية وتصوير المواقع والتحركات السورية العسكرية.

بعد الغزو السوفيتي لأفغانستان المسلمة بفترة وضع السوفيت سفينة في بحر العرب للتشويش المخادع على إذاعة الـ (BBC) الإنجليزية إذ كانت تلك الإذاعة تذيع أخبار أفغانستان باللغة البلوشستيه في وقت ثابت لمدة ساعتين يوميا وكانت معظم الأخبار صحيحة ، فعمد السوفيت إلى التشويش على إرسال الإذاعة في منطقة أفغانستان وكذلك ببث أخبار غير صحيحة من على ظهر السفينة، بصوت يقارب صوت مذيع الـ

(١) كتاب : INTELLEGENCE WARFARE ص ١٢٤ .

(BBC) وبذبذبة قرب ذبذبة الإذاعة الإنجليزية المشوش عليها وذلك لإثارة البلبلة في نفوس المجاهدين الأفغان، وليتخذوا على أساسها إجراءات قد تكون في غير صالحهم.

في حرب فوكلاند :

١ ـ إستحدث الإنجليز إذاعة جديدة توجه إرسالها إلى الأرجنتين يوميا باللغة الإسبانية المستعملة في الأرجنتين لخلق حالة نفسية سيئة لدى الشعب الأرجنتيني، وزعزعة ثقته في قواته المسلحة.

٢ ـ وبنفس الطريقة بث الأرجنتينيون إذاعة يوميا موجهة إلى القوات الإنجليزية تذيع باللغة الإنجليزية دعاية لصالحهم وموسيقى صاخبة وموسيقى قروية قديمة إنجليزية لتشوق الإنجليز إلى العودة لوطنهم كما بثت أخبار تبين فيها أن جزيرة فوكلاند أصلا تابعة للأرجنتين وأن الإنجليز مغتصبوها وأن المسافة بعيدة جداً من إنجلترا. لذا فمن المؤكد أن إنجلترا ستخسر أموالا طائلة في هذه الحرب وأنها في ضائقة مالية بالإضافة إلى الخسائر العسكرية الفادحة وذلك للإستعداد الكامل للأرجنتين وبعد المسافة بين فوكلاند وإنجلترا. . الخ.

٣ ـ أدى سوء الإستطلاع الجوي الإنجليزي وعدم دقة التصوير الجوي من خلال الطائرات الإستطلاعية وعدم إستخدام القمر الصناعي بسبب وجود غيوم كثيفة فوق فوكلاند، وأدى ذلك إلى أن القاذفات الإنجليزية عندما قصفت مطار بورت ستانلي (PORTSTANLY) مرتين كان القصف غير دقيق، وحتى بعد القصف الثاني إستطاع الأرجنتيون استخدام المطار وإنقاذ الطائرات المتبقية من القصف.

٤ ـ علمت الأرجنتين أن البارجة تشفيليد الإنجليزية إذا أرادت الإتصال عبر الأقمار الصناعية أو عبر (HF RADIO) مع القيادة في إنجلترا فإنها تطفيء رادار السفينة، وفي هذه الحالة لا تكتشف السفينة الصواريخ البعيدة الموجهة إليها وكانت هناك طائرة سوبر اتندار أرجنتينية محملة بصواريخ (EXOCET) تراقب ذلك وعندما أطفأ الإنجليز الرادار للإتصال بإنجلترا أطلق الصاروخ وأصاب تلك السفينة إصابة مدمرة[1].

---

(١) مجلة FLIGHT INTERNATIONAL عدد ١٩٨٢/٧/١٠ م ص ٦٦.

عندما كانت السفينة نيوجرزي (NEW JERSY) ذات المدافع الضخمة تهدد وتقصف منطقة بيروت كانت تصاحبها سفينة (CARON) الخاصة بمعدات الحرب الإلكترونية (E. W. SHIP) والتي تقوم بمراقبة المياه القريبة لكي تحمي السفينة نيوجيرزي من المهاجمات خصوصا المفاجئة مثل الضفادع البشرية.

أوردت بعض المصادر أن الأمريكان هم الذين أرادوا جعل الطائرة الكورية البوينج ٧٤٧ تنحرف عن مسارها في سبتمبر ١٩٨٣ لتقترب من القاعدة السوفيتية الرئيسية في شمال شرق آسيا لكي يشغل السوفيت أجهزتهم المتطورة في تلك القاعدة للتصدي لهذا الهدف ومن ثم تلتقط الأقمار الصناعية وطائرات التنصت وسفن التنصت الأمريكية الموجودة في المكان جميع الموجات الكهرومغناطيسية المنبعثة من الأجهزة السوفيتية لتحليلها ومعرفة خواصها ثم تصنيع أجهزة مضادة لها، وقد قيل أن أمريكا استطاعت التقاط أوامر إطلاق النار الروسية على الطائرة الكورية ولكنها كانت مشفرة فبعثت إلى أمريكا فورا للتحليل وبعد ٤ ساعات استطاعوا معرفة المعلومات المشفرة بأجهزة التحليل ولكن بعد فوات الأوان إذ أسقط السوفيت الطائرة الكورية.

أنتجت بعض الدول المتقدمة أخيرا نوعا جديدا من القنابل يعمل على تكوين كتلة كبيرة من الغمام المتأين المليء بالإلكترونات، وتحلق تلك الغمامة على ارتفاع شاهق فوق الدول المعادية، لتقوم بعكس الموجات (خاصة VHF/ UHF) كي تستطيع الدول المتقدمة التقاطها وتحليلها والإستفادة منها. وتمكث هذه الغمامة بضع ساعات ثم تهبط إلى الأرض بفعل الجاذبية الأرضية.

تتعمد إسرائيل إطفاء أجهزتها ذات البث اللاسلكي مثل الرادارات وأجهزة الإتصالات.. الخ أثناء مرور الأقمار الصناعية التجسسية السوفيتية فوق أراضيها حتى لا ترصدها تلك الأقمار وتعرف خواصها، كما أنها تتعمد إطفاء المولدات الكهربائية الموجودة في الأماكن النائية التي تمد مواقعها العسكرية وخاصة بطارياتها العسكرية بالكهرباء وذلك خوفا من التصوير بالأشعة تحت الحمراء (INFRARED SENSORS) التي تملكها الأقمار الصناعية السوفيتية.

معركة وادي البقاع الإلكترونية

سنعرض هنا دور الحرب الإلكترونية في معركة وادي البقاع اللبناني بين الجيش السوري والجيش الإسرائيلي في ٩، ١٠ يونيو عام ١٩٨٢م.

لقد حدثت كارثة طيران في وادي البقاع اللبناني في ٩، ١٠ يونيو عام ١٩٨٢[١] عندما استطاعت إسرائيل إسقاط حوالي مائة طائرة حربية سورية وتدمير حوالي ١٧ بطارية سام ـ ٦ من أصل ٢٠ بطارية، تبعها بعد ذلك بفترة تدمير عدد ٢ بطارية صواريخ سام ـ ٨ وعدد ١ بطارية صواريخ سام ـ ٥ تابعة للجيش السوري.

لاشك أن إسقاط مائة طائرة حربية وتدمير ١٧ بطارية سام ـ ٦ في ظرف يومين تعتبر كارثة عسكرية، علما بأن هذه المعركة كانت معركة محدودة وليست شاملة، لكن هذه النتائج لم تأت بمجرد الصدفة أو بتفوق الطيران الإسرائيلي وأسلحته التقليدية (CONVENTIONAL WEAPONS) وإنما صاحب هذه إعتماد كبير على أجهزة وأساليب الحرب الإلكترونية وهذا النوع من الأجهزة تقوم إسرائيل بتصنيعه، فقد إستخدمت إستخبارات الإشارة (SIGINT) والإجراءات الإلكترونية المساندة ESM) والإجراءات الإلكترونية المضادة (ECM) ولابد أيضا أن نذكر أن بعض الأجهزة الإلكترونية التي استعملت في معركة وادي البقاع اللبناني كانت أجهزة إسرائيلية الصنع وكان لها دور فعال، وخاصة الطائرات التي تطير بدون طيار (DRONES AND R. P. VS) من نوع (MASTIF) وهي من إنتاج شركة تاديران ـ شركة الصناعات الإلكترونية الإسرائيلية المحدودة (TADIRAN, ISRAEL ELECTRONICS INDUSTRIES LTD) ـ ونوع (SCOUT) وهي من إنتاج شركة صناعة الطائرات الإسرائيلية المحدودة (ISRAEL AIRCRAFT INDUSTRIES LTD) واللتين كانتا محملتين بأجهزة إسرائيلية من كاميرات تصوير وكاميرات

---

(١) مجلة FLIGHT INTERNATIONAL تاريخ ١٩/٦/١٩٨٢م و٩/٣/١٩٨٥م ص ١٥٩٦ ص١٠.

تلفزيونية وأجهزة (COMINT, ELINT, ESM, ECM) وقد ذكر الدكتور أزيو بونسفنور، وهو إيطالي الجنسية، في عدد خاص من مجلة حلف الناتو صدر عام ١٩٨٢، أن إسرائيل أيضا استخدمت طائرات أخرى بدون طيار تسمى «دليلة» تنطلق من طائرة الفانتوم (F-4) وكانت تلك الطائرات الصغيرة الحجم تقوم بتصوير المواقع السورية المعرضة للقصف وتنقلها إلى مركز القيادة لتصحيح أخطاء القصف الإسرائيلي على تلك المواقع، كما قال الدكتور أزيو أيضا أن تلك الطائرات كانت تنقل على الهواء مباشرة وقائع إسقاط الطائرات وتدمير بطاريات سام ـ ٦ السورية في تلك المعركة، فكانت تنقل الوقائع تلفزيونيا مباشرة إلى مركز العمليات العليا في وزارة الدفاع الإسرائيلية في تل أبيب.

وكما قلنا لم تأت نتائج تلك المعركة بطريق الصدفة وإنما لها تاريخ من التخطيط والمراقبة والإستطلاع والتدريب النظري والعملي باستخدام أجهزة الحرب الإلكترونية، وكما سبق أن ذكرنا فإن تدريبهم على قصف المفاعل النووي العراقي في ١٩٨١/٥/٧ استغرق عدة شهور قبل تنفيذ العملية.

ولكي نتصور هذا التخطيط وهذه الدراسة لتلك المعركة التي أدت إلى هذه النتائج الوخيمة. علينا أن نرجع إلى بعض التواريخ لنرى تطور الأمر :

١ ـ فقدت إسرائيل في الثلاثة أيام الأولى من حرب ١٩٧٣ حوالي ١٥٠ طائرة حربية معظمها أسقط بصواريخ سام ـ ٦، بعد ذلك زودت أمريكا إسرائيل أثناء الحرب بأجهزة تشويش لتشوش على تلك الصواريخ وأدى هذا إلى انخفاض حاد في عدد الطائرات الإسرائيلية التي تدمرها الصواريخ العربية(١) وبهذا تعلمت إسرائيل درسا لن تنساه في موضوع الحرب الإلكترونية.
وقد قالت بعض المصادر البريطانية أن استعمال إسرائيل لأجهزة التشويش غير الموازين نسبياً في تلك الحرب، حيث استطاعت إسرائيل الحصول على بعض صواريخ سام ـ ٦ بحالة جيدة فعرفت خواصها وأسرارها(٢).

٢ ـ استطاع بعض الإسرائيليين التسلل إلى سوريا ووضع بعض أجهزة المراقبة والتنصت في خط الإتصال الذي يربط بين سوريا والأردن .

---

(١) انظر مجلة الوطن العربي التي تصدر في باريس تاريخ ١٩٨٢/١٠/١م.
(٢) مجلة الوطن العربي ١٩٨٢/٥/١م.

وهي نتاج صناعة مشتركة بين شركة (ELECTRONIC) الأمريكية وشركة (TADIRAN) الإسرائيلية .

٣ ـ في أكتوبر عام ١٩٧٩ أرسلت إسرائيل طائرة إستطلاع، بدون طيار فوق سوريا لتستطلع بعض الحشود السورية، وقد إعترفت إسرائيل بذلك.

٤ ـ في عام ١٩٨١ إستطاعت سوريا إسقاط حوالي ٩ طائرات استطلاعية بدون طيار فوق وادي البقاع اللبناني وفوق الأراضي السورية قرب دمشق.

٥ ـ تعمدت إسرائيل إرسال طائرات بدون طيار إلى وادي البقاع كطعم (DECOY) لكي يشغل السوريون الرادار الموجه لصواريخ سام ـ ٦ وفعلا حدث ما أرادت ففي نفس اللحظة حلقت طائرتان إسرائيليتان استطلاعيتان تحليقا عاليا جدا لإلتقاط ذبذبات وموجات ذلك الرادار، لكي يقارن الإسرائيلون خواص رادارات صواريخ سام ـ ٦ هذه بالتي كانت مستعملة في حرب ١٩٧٣، وأيضا لمعرفة كافة المعلومات عن تلك الرادارات كي يتمكنوا من التشويش عليها .

٦ ـ أسقطت سوريا طائرة استطلاع بدون طيار في وادي البقاع في أوائل ١٩٨٢ .

هذا عدا الطائرات الإسرائيلية الحربية الإستطلاعية والطائرات الإستطلاعية بدون طيار التي لم ترها سوريا ولم تسقطها.

وحتى نعطي تصورا عن معركة وادي البقاع اللبناني، ومن ثم نضع سيناريو تحركات القوات الإسرائيلية التي حطمت ودمرت الطائرات والصواريخ السورية، يجب أن نشير إلى بعض التقارير المؤرخة والمأخوذة من عدة مصادر :

١ ـ تبين أن هناك إتفاقا قديما مبرما بين الولايات المتحدة الأمريكية وإسرائيل يقضي بأن تحصل إسرائيل على بعض المعلومات التي ترسلها الأقمار الصناعية الأمريكية.

٢ ـ في معركة وادي البقاع اللبناني أرسلت الولايات المتحدة الأمريكية إلى إسرائيل طائرة أواكس وبعض المعلومات التي حصلت عليها الإستخبارات الأمريكية، وذلك لتساعد إسرائيل في تلك المعركة.

٣ ـ إتضح أن مواصفات صواريخ سام ـ ٦ المستعملة في معركة وادي البقاع هي نفس مواصفات سام ـ ٦ المستخدمة في حرب ١٩٧٣ لم يطرأ عليها أي تعديل.

٤ ـ أن إسرائيل استخدمت تقنيات الحرب الإلكترونية المتطورة، واستخدمت طائرات بوينغ ٧٠٧ المزودة بأجهزة الحرب الإلكترونية. (E.W. A/C « ELECTRONIC WARFARE AIRCRAFT) وإستخدمت عدد ٤ طائرات من نوع عين الصقر (HAW-KEYE E-2C) للإنذار المبكر.
وكذلك إستخدمت النصلات (CHAFF) ، كل هذا استخدمته إسرائيل في معركة وادي البقاع اللبناني في عام ١٩٨٢م.(١)

٥ ـ ذكر في أحد التقارير أنه أثناء المعركة كانت هناك سفن أمريكية استعملت للتشويش على أجهزة القوات السورية.

٦ ـ ويقول تقرير آخر أن إسرائيل استخدمت نظام القيادة والسيطرة الأمريكي بموافقة أمريكية في معركة وادي البقاع، ونظام القيادة والسيطرة الأمريكي هو:
مراقبة كل ما يجري على وجه الأرض، وهو نظام للكشف والإنذار متطور جداً تتم فيه جمع المعلومات المأخوذة من:
أ ـ الأقمار الصناعية والمكوكات الفضائية.
ب ـ طائرات الإنذار المبكر المحلقة مثل الأواكس وعين الصقر.
جـ ـ أجهزة التنصت والرصد الأرضية المنتشرة.
كل هذه المعلومات تصب في مركز القيادة الأمريكية العليا في إحدى الولايات المتحدة.

٧ ـ ذكرت مجلة الوطن العربي التي تصدر في باريس في عددها الصادر بتاريخ ١٩٨٢/١١/١٠:
نقلا عن مصادر غربية أن إسرائيل استخدمت في تلك المعركة:
أ ـ طائرات بدون طيار تسمى «شمشون» تطلق من طائرات الفانتوم (F-4) ونوعا آخر يسمى «دليلة» يطلق من الأرض، وكلاهما لخداع الرادارات الأرضية ورصد جميع المعلومات المنبعثة من رادارات صواريخ سام ـ ٦.
ب ـ طائرات تنصت من نوع بوينغ ٧٠٧ أمريكية توجد بها أجهزة (ESM) لمراقبة مواقع رادارات سام ـ ٦ وأجهزة أخرى للتشويش (ECM)(٢).

---

(١) مجلة AVIATION WEEK AND SPACE TECHNOLOGY عدد ١٩٨٢/٧/٥م ص١٦.
(٢) المصدر السابق صفحة ١٧ .

جـ ـ طائرات عين الصقر للإنذار المبكر (E-2C)
د ـ طائرات هيلوكبتر كبيرة نوع (CH-35) تحمل أجهزة تشويش ضد رادارات سام ـ ٦ .
هـ ـ أجهزة تشويش أرضية موجودة على مرتفعات عالية تطل على وادي البقاع اللبناني لكي تشوش على رادارات صواريخ سام ـ ٦ والطائرات الحربية السورية .
و ـ وكذلك استخدمت الفانتوم (F-4) لتدمير مواقع سام ـ ٦ بقنابل عنقودية[1] .

٨ ـ قبل المعركة بأسابيع قليلة إستطاع الإسرائيليون تدمير محطة رادار سورية للإنذار المبكر في خلدة على الساحل اللبناني لكي تكون أية طائرة إسرائيلية تقترب من وادي البقاع في مأمن من الكشف والإنذار السوري ولم تقم سوريا بتجديد محطة رادارات الإنذار المبكر المدمرة.

والآن بعد سرد بعض التقارير التي نـاقشت ظروف تلك المعـركة ، سنستعـرض سيناريو الأحداث من بداية المعركة حتى نهايتها الكترونيا لنتصور مدى استخدام إسرائيل لأساليب وأجهزة الحرب الإلكترونية .

أولا : جمعت إسرائيل كل المعلومات عن أسلحة سوريا ومواقعها في وادي البقاع وخاصة صواريخ سام ـ ٦ ، وكانت مصادر تلك المعلومات كثيرة منها:

المعلومات المأخوذة من الطائرات الإستطلاعية (خاصة التي تطير بدون طيار)، والأقمار الصناعية الأمريكية، وطائرات الإنذار المبكر مثل الأواكس الأمريكية وعين الصقر (E-2C) الإسرائيلية وطائرة الحرب الإلكترونية البوينغ ٧٠٧، والإستخبارات الأمريكية والإستخبارات الإسرائيلية فحللت إسرائيل تلك المعلومات واستفادت منها ودربت العسكريين الإسرائيليين على استخدام الطائرات مع أجهزة الحرب الإلكترونية لتلك المعركة.

ثانيا : أرسلت إسرائيل طائرة أو عدة طائرات من عين الصقر (E-2C) في البداية لكي تحلق فوق البحر المتوسط بين بيروت وقبرص لمراقبة جميع التحركات في المنطقة عن

---

(١) مجلة الوطن العربي ١/١٠/١٩٨٢.

بعد وخاصة « الطائرات السورية في قواعدها في سوريا »، كما أرسلت طائرة الأواكس الأمريكية وطائرة الحرب الإلكترونية البوينغ ٧٠٧ (E. W. AIRCRAFT) وطائرات الهيلوكبتر المشوشة فوق أجواء لبنان.

ثالثاً : أطلق الإسرائيليون نوعين من الطائرات الصغيرة بدون طيار(DRONES & R. P. V.).

النوع الأول : طائرة SCOUT الإسرائيلية :

وتستعمل كطعم لرادارات سام ـ ٦ لتظهر عند مشغل رادار البطارية وكأنها أهداف كبيرة فيشغل رادار موجه الصواريخ (FIRE CONTROL RADAR) وفعلا شغل السوريون تلك الرادارات وأطلقوا صواريخ سام ـ ٦ باتجاه هذه الطائرات وزعم السوريون بعدها أنهم أسقطوا ١٩ طائرة إسرائيلية مقاتلة في حين أنها كانت من طائرات (SCOUT) (الطعم).

والنوع الثاني طائرة MASTIF الإسرائيلية :

وهذا النوع من الطائرات يختلف في خواصه عن النوع الأول إذ من الصعب ملاحظته على شاشات الرادار حتى تستطيع الطائرة التحليق بدون مضايقة لتصور المواقع السورية في وادي البقاع. مرسلة هذا التصوير في نفس اللحظة بالموجات اللاسلكية إلى مركز القيادة الإسرائيلية ليراقب الإسرائيليون ما يحدث وليصححوا إتجاه القصف على المواقع السورية، وكما ذكرنا في أول هذا الفصل أن تلك الطائرات كانت تنقل أحداث المعركة نقلا تلفزيونيا مباشرا إلى مركز العمليات الإسرائيلي الأعلى في وزارة الدفاع في تل أبيب، ويقال أن بعض هذه الطائرات وضعت بها قنابل شديدة الإنفجار، لتسقط على المواقع السورية وتدمرها.

رابعا : في هذه الأثناء تكون طائرة الأواكس الأمريكية أو طائرة الحرب الإلكترونية البوينغ ٧٠٧[1] (E.W. AIRCRAFT « ESM, & ECM ») قد رصدت ذبذبات

---

(١) مجلة AVIATION WEEK AND SPACE TECHNOLOGY عدد ١٩٨٢/٧/٥ صفحة ١٦.
وكذلك مجلة FLIGHT INTERNATIONAL عدد ١٩٨٥/٣/٩م ص١٠. «وادعت المجلة أن تلك الطائرة البوينغ ٧٠٧ قد شوشت كذلك على إتصالات السوريين».

وموجات صواريخ سام ـ ٦ وبثتها إلى طائرة التشويش الهليوكبتر الكبيرة (CH-35) ومحطات التشويش الأرضية على جبل الباروك في لبنان فتعمل جميعها (البوينغ ٧٠٧ والهيلوكبتر (CH-35) والمحطات الأرضية) للتشويش على جميع الرادارات والإتصالات السورية في وادي البقاع ولتشله إلكترونيا، وكانت أجهزة التشويش تعمل بطريقة (STAND-OFF-JAMMING) (أي العمل خارج مجال الصواريخ والقوات المعادية بغير إشتراك فعلي في المعركة).

خامساً : أقلعت في نفس الوقت ٩٠ طائرة إسرائيلية من نوع فانتوم وسكاي هوك (A-4) وإف ـ ١٦ وإف ـ ١٥ . وقد حلقت جميعها في تشكيل متقارب فوق وادي البقاع لكي تربك رادارات وصواريخ سام ـ ٦ لكثرة إنعكاس الموجات الرادارية وهذا يؤدي مع التشويش الجوي والأرضي إلى تعمية رادارات وصواريخ سام ـ ٦ حيث يؤدي هذا بدوره إلى ضعف أداء صواريخ سام ـ ٦ أو عدم إنطلاقها من مواقعها.

سادسا : يقوم سرب الفانتوم (F-4) وسكاي هوك (A-4) بتحليق منخفض محتميا خلف سلسلة جبال لبنان الغربية وبين الوديان مقتربا من مواقع الصواريخ ثم فجأة يحلق عاليا الواحدة تلو الأخرى بطريقة (PUP-UP) ملقية قنابل عنقودية CLUSTER BOMBS) (« BLUE 72 » على تلك الصواريخ لتدمرها، كما يقوم سرب طائرات إف ـ ١٦ (أو إف ـ ٤ فانتوم) المزودة بصواريخ جو ـ أرض من نوع (SHRIKE) المضادة للرادارات الأرضية بتدمير رادارات صواريخ سام ـ ٦، كما إستخدمت إسرائيل صواريخ أرض ـ أرض (« WOLF » NEWZEEV) الإسرائيلية المضادة لرادارات الدفاع الجوي للقيام بالمهمة نفسها[١].

سابعا : ولابد هنا أن تقلع طائرات سورية مقاتلة للنجدة ولتدارك الأمر وانقاذ المواقع السورية، وفي هذا الوقت تقوم طائرة (أو طائرات) عين الصقر (E-2C) الإسرائيلية بمراقبة المطارات السورية عن بعد وعند إقلاع الطائرات السورية تعطي الطائرات الإسرائيلية جميع المعلومات أولا بأول للسرب الباقي من الطائرات التسعين وهي طائرات إف ـ ١٥ وإف ـ ١٦ وهذه الطائرات مزودة بصواريخ جو ـ جو من نوع (SIDE WINDER) الأمريكية لكي تلاحق الطائرات السورية الآتية للنجدة وتسقطها وفي نفس الوقت تستقبل طائرة الحرب الإلكترونية الإسرائيلية البوينغ ٧٠٧ جميع الموجات

(١) مجلة AVIATION WEEK AND SPACE TECHNOLOGY تاريخ ١٩٨٢/٧/٥ صفحة ١٦و ١٧.

الكهرومغناطيسية المنبعثة من أجهزة الإتصالات والرادارات والأجهزة الملاحية الموجودة بالطائرات السورية وبثها إلى طائرات الهليوكبتر والمحطات الأرضية المشوشة التي تقوم هي الأخرى بالتشويش على جميع أجهزة الطائرات السورية، وبهذه الحالة يكون الطيار السوري حالما يدخل الأجواء اللبنانية في حالة «عمى إلكتروني» (ELECTRONIC BLACKOUT) فلا يستطيع تلقي التوجيهات من الرادارات السورية الأرضية ولا من قائد السرب ولا من رادار طائرته ولا حتى من أجهزة الطائرة الملاحية، فقط يستطيع النظر من خلال زجاج النافذة وهذه الحالة غاية في الخطورة إذا كان في مهمة قتالية، وبذلك تكون الطائرات السورية لقمة سائغة لطائرات إف ـ ١٥ المتطورة (وإف ـ ١٦).

وحينئذ يجب أن لا نتعجب من خسائر تلك المعركة التي كانت كالتالي :

سقوط حوالي مائة طائرة سورية معظمها ميج ٢١ و٢٣ وتدمير ١٧ بطارية سام ـ ٦ من أصل ٢٠ بطارية ويقال أن عدد ١٠ بطاريات سام ـ ٦ حطمت خلال الدقائق العشر الأولى من المعركة، ولم يخسر الجانب الإسرائيلي في تلك المعركة إلا بضع طائرات صغيرة بدون طيار وطائرة هيلوكبتر واحدة يقال أنها أسقطت بطريقة الخطأ(١). ويقال أن هناك أيضا تحطمت صواريخ سورية سام ـ ٢ وسام ٣ في نفس المعركة(٢) وكذلك المدافع المضادة للطائرات من نوع شيلكا (SHILK A ZSU-23-4)(٣)

وقد دهشت إسرائيل لهذه النتائج الكبيرة وخاصة ضد المدافع المضادة للطائرات التي كان نصيبها في تحطيم الطائرات الإسرائيلية في حرب ١٩٧٣ يعادل ٥٥٪(٤).

هذا وقد نبهت صحيفة النهار اللبنانية إلى هذه الكارثة قبل عام من حدوث المعركة وكيفية تدمير صواريخ سام ـ ٦ في وادي البقاع، بعددها الصادر بتاريخ ١٣/٥/١٩٨١ وكذلك صحيفة السفير اللبنانية الصادرة بنفس التاريخ.

كما حذر رئيس الوزراء الإسرائيلي مناحيم بيغن من تلك المعركة وذلك في مقابلة إذاعية معه أجرتها إذاعة الجيش الإسرائيلي . . قبل حدوث المعركة بحوالي شهرين إذ قال أن إسرائيل ستدمر الصواريخ السورية في وادي البقاع اللبناني إذا اعترضت الطائرات

---

(١) مجلة الوطن العربي ١/١٠/١٩٨٢.

(٢) مجلة FLIGHT INTERNATIONAL عدد ٢١/٨/١٩٨٢ ص٤٠٤.

(٣) مجلة AVIATION AND SPACE TECHNOLOGY عدد ٥/٧/١٩٨٢ صفحة ١٧.

(٤) مجلة MILITARY TECHNOLOGY عدد يوليو ١٩٨٢م صفحة ١١٠.

السورية الطائرات الإسرائيلية فوق لبنان، وقال أيضا:

إذا هاجم الفدائيون الفلسطينيون الإسرائيليون المدنيين داخل إسرائيل فسندخل لبنان ونطرد جميع الفدائيين منها.

وأخيراً يقول تقرير نشرته جريدة القبس الكويتية:

إن سبب هزيمة السوريين أمام الإسرائيليين في معركة وادي البقاع اللبناني في عام ١٩٨٢ هو تفوق الجيش الإسرائيلي من حيث استخدام أساليب وأجهزة الحرب الإلكترونية المتطورة، وقد أيد ذلك تصريح وزير الدفاع السوري في مقابلة مع مجلة دير شبيغل[٢] ولم تكن هذه المعركة هي نهاية المطاف بل عزز السوريون موقفهم وناشدوا الإتحاد السوفيتي بإعطائهم أسلحة متقدمة لمواكبة تطور أجهزة وأساليب الحرب الإلكترونية حتى لا تتكرر كارثة معركة وادي البقاع، وقد أدرك قادة الإتحاد السوفيتي ذلك فبعثوا بضباط متخصصين في الحرب الإلكترونية بعد تلك المعركة بفترة وجيزة، وأعطوا السوريين صواريخ سام ـ ٨ وصواريخ سام ـ ٦ كما زودوهم بصواريخ سام ـ ٥ ذات المدى البعيد (حوالي ٣٠٠ كم) لمواجهة طائرات الإنذار المبكر الإسرائيلية عين الصقر (E-2C).

وهذه طائفة من التقارير حول المساعدات الروسية لسوريا :

١ ـ يذكر أحد التقارير أن الإتحاد السوفيتي أعطى سوريا طائرات إنذار مبكر تشبه طائرات الأواكس الأمريكية.

٢ ـ بعد معركة وادي البقاع اللبناني زود الإتحاد السوفيتي سوريا بصواريخ سام ـ ٨، ووضعت سوريا بعض من تلك الصواريخ في لبنان وإستطاعت إسقاط عدة طائرات فانتوم.

٣ ـ وتقرير آخر يقول: أنه يوجد حوالي ٥ آلاف خبير روسي في سوريا يعملون بشبكة صواريخ سام ـ ٥، والشبكة متصلة مع القيادة السوفيتية العليا في موسكو عبر الأقمار الصناعية.

٤ ـ وسوريا هي أول دولة في العالم تحصل على صواريخ سام ـ ٥.

---

(٢) مجلة دير شبيغل الألمانية الغربية (من جريدة القبس تاريخ ٢٥/١٠/١٩٨٤ م).

٥ ــ أما إسرائيل فتقول أنه قد تم ربط القيادة العليا السورية مع القيادة العليا الروسية عبر الأقمار الصناعية. لكن حسب ما جاء في جريدة القبس الكويتية الصادرة بتاريخ ١٩٨٣/٦/٢٠م: فإن أوامر إطلاق صواريخ سام ـ ٥ السورية تصدر عن الروس في موسكو عبر الأقمار الصناعية.

لكن هذا التطور والتعزيز من الجانب السوري لم تغفل عنه إسرائيل، فقد استمرت في نشاطها الإستطلاعي وتهديداتها لتؤكد للجميع أن التفوق والسيطرة مازالا بيدها:

١ ــ إن إسرائيل دمرت عدد ٣ بطاريات سام ـ ٨ الجديدة السورية في ١٩٨٢/٧/٢٤[1] (عندما أرادت القوات السورية تحريكها إلى مكان آخر وقد عرفت إسرائيل أن انتقال أو تحرك بطارية سام ـ ٨ بهذه الصورة يجعلها غير قادرة على العمل وإطلاق الصواريخ نحو الأهداف):.

٢ ــ يقول وزير الدفاع الإسرائيلي موشيه ايرنز أن لدى إسرائيل الآن الأجهزة المناسبة (ECM) للتشويش على صواريخ سام ـ ٥ وقد أيده بعد ذلك خبير غربي في تقرير له.

٣ ــ أفاد أحد الخبراء العسكريين أن أمريكا أعطت إسرائيل صواريخ بعيدة المدى مضادة لصواريخ سام ـ ٥ التي تمتلكها سوريا، وتطلق هذه الصواريخ من البحر الأبيض المتوسط.

٤ ــ تؤكد إسرائيل أن عندها الآن الأجهزة المناسبة للتشويش وإعاقة سام ـ ٥.

٥ ــ تفكر إسرائيل بجدية في توجيه ضربة وقائية ضد صواريخ سام ـ ٥ السورية.

٦ ــ تفيد المصادر أن أمريكا زودت إسرائيل بصور وأخبار سرية من الأقمار الصناعية الأمريكية عن شبكة الإنذار المبكر السورية.

٧ ــ أسقطت سوريا بعد ذلك عدة طائرات إستطلاعية بدون طيار فوق لبنان، وذكر أن إسرائيل تعمل بنشاط لوضع شبكة طائرات إستطلاعية قرب وادي البقاع اللبناني.

٨ ــ وفي ١٩٨٣/١٢/٦ أسقطت سوريا طائرتين استطلاعيتين إسرائيليتين فوق وادي البقاع اللبناني.

---

(١) مجلة FLIGHT INTERNATIONAL عدد ١٩٨٢/٨/٧ صفحة ٢٩١.

٩ ـ أفادت بعض المصادر أن أمريكا قد أتمت تطوير الطائرات الإسرائيلية إف ١٥ وإف ١٦ وأصبحت الآن مزودة بأحدث أجهزة الحرب الإلكترونية .

ومن هنا نرى أن أجهزة وأساليب الحرب الإلكترونية ـ كبقية الأسلحة ـ تتطور بين فترة وأخرى وتجعل الذين لا يواكبون تطورها في عداد الخاسرين عسكرياً .

الباب الخامس

متطلبات أساسية للحرب الالكترونية

نوجز هنا بعض المتطلبات الأساسية للحرب الإلكترونية، سواء المتطلبات الخاصة باستحداث مثل هذا المجال أو الخاصة بالمراحل التالية أثناء العمل، والتي تعتبر ضرورية وتؤثر تأثيرا مباشرا على نجاح هذا المجال في تحقيق أغراضه وأهدافه.

١ ــ مكتبة التهديدات :

ويقصد هنا بمكتبة التهديدات أي جميع المعلومات التي تفيد في معرفة إمكانات وقدرات وأسلحة العدو المختلفة، وتحديد نقاط الضعف والقوة لأسلحته ومعداته وبالتالي معرفة تهديداته ونواياه الممكنة، والذي يقود إلى اختيار الخطة المناسبة للدفاع أو الهجوم ووضع التخطيط المناسب والتنبؤ باحتياجاتنا المستقبلية.

(١) الهدف الأساسي لهذه المكتبة هو التجميع وفرز وتنسيق وتحليل المعلومات المزودة عن طريق استخبارات الإشارة أو غيرها من الجهات المساندة، للاستفادة منها في الأغراض التالية:

أ ــ إختيار نوعية أساليب وأجهزة الإجراءات الإلكترونية المضادة (ECM) واجراءات الحماية الإلكترونية (ECCM) وكيفية برمجتها واعدادها والتدريب عليها .

ب ــ الإسهام في وضع خطط العمليات الحربية.

جـ ــ الإسهام في التخطيط للاحتياجات المستقبلية.

(٢) إن إعداد هذه المكتبة يتطلب خبرة وجهداً كبيراً ووقت طويل من العمل المتواصل في جمع المعلومات وتحديثها وإدامتها. ويجب أن نلفت الإنتباه إلى أن مصادر هذه المكتبة لا يقتصر على معدات استخبارات الإشارة والإجراءات الإلكترونية المساندة بل إلى مصادر أخرى مثل:

أ ــ معدات التصوير الكهروبصرية والمستخدمة للأشعة الحمراء أو الرادارية أو

معدات التصوير البصرية.

ب ـ الكتب والنشرات الدورية.

جـ ـ الدول الصديقة.

د ـ الجواسيس.

هـ ـ الشركات المصنعة.

٣ ـ خطوات العمل لتكوين مكتبة التهديدات :

أ ـ جمع المعلومات وتحليلها.

ب ـ ترتيب وتخزين المعلومات بشكل جيد ومنسق يضمن سرعة إستخراجها عند الطلب للإضافة أو الإلغاء أو التغيير أو الإستفادة.

جـ ـ ربط المعلومات فيما بينها ووضع تصور عام ومختصر عن العدو.

د ـ مناقشة المعلومات الحديثة والقديمة من الناحية التعبوية والفنية ومن الناحية الإستخبارية للوصول إلى تقدير موقف متكامل عن إمكانيات العدو وخططه.

هـ ـ وضع الحلول المناسبة من حيث التدريب والتجهيز والتأهب للهجوم أو الدفاع.

وباستخدام معلومات مكتبة التهديدات (أو مكتبة الحرب الإلكترونية كما تسمى أحيانا) من قبل المختصين في الحرب الإلكترونية والمعنيين من العمليات الحربية يتم إعداد واتخاذ قرار إلكتروني (E.W. SUPPORT ACTION) في العمليات الحربية بشكل متكامل وفعال.

٢ ـ الموقف الإلكتروني للمعركة :

ELECTRONIC ORDER OF BATTLE (E.O.B.)

وهو يعتبر المعلومات المجمعة عن الموقف الحربي الإلكتروني عن قوات العدو وقواتنا وتكون مصدر هذه العمليات من مكتبة التهديدات وقد تعد وتحفظ في مكتبة التهديدات نفسها.

١ ـ الموقف الإلكتروني للعدو :

وهو كل ما يتعلق بإمكاناته الإلكترونية من مراقبة وتشويش وحماية وإستخبارات، وكذلك إمكاناته من معدات الإتصالات ومعدات غير الإتصالات والأسلحة وذلك من حيث :

أ ـ أنواع وأعداد المعدات والأسلحة.

ب ـ مواقعها.

جـ ـ إمكاناتها وقدراتها ومواصفاتها.

د ـ مهارة المستخدمين لها.

هـ ـ الصلاحية وأوقات الصيانة والتشغيل والإغلاق.

و ـ مدى الإستفادة منها في الهجوم.

ز ـ مدى الإستفادة منها في الدفاع.

ح ـ البدائل الموجودة كأنظمة أو معدات أو تعليمات.

ط ـ نقاط الضعف والقوة.

ي ـ التنسيق وطرق الربط.

ك ـ الترددات المستخدمة ومواصفات الموجات الكهرومغناطيسية.

٢ ـ الموقف الإلكتروني لقواتنا :

ويتضمن كل ما جاء في البند (١) ولكن بالنسبة لقواتنا، ولو بشكل مختصر ومبسط، ويعد هذا الكتاب بتصنيف سري للغاية ويرفع للقائد.

٣ ـ تنظيم أقسام الحرب الإلكترونية :

يقصد به تقسيم مهام وعمليات الحرب الإلكترونية لأقسام معينة، ووضع سياسات التنسيق فيما بينهم وذلك على جميع مستويات القوات المسلحة، وذلك لضمان توفير الجهود والأموال وتحديد السلطات والإختصاصات. ويعتبر التنظيم أول العناصر التي يجب البدء بها عند التفكير بإنشاء الحرب الإلكترونية، وتحتاج عملية التنظيم إلى خبرة طويلة، إلا أن وضع التنظيم ولو بشكل مبدئي يحفظ الجهود من التشتت.

(١) أمور يجب أخذها بعين الإعتبار عند وضع تقسيمات الحرب الإلكترونية.

(أ) إن معدات وأساليب (SIGINT, E.S.M, E.C.M) تحتاج إلى أقسام خاصة وقوى بشرية متفرغة ومتخصصة في أساليب ومعدات الحرب الإلكترونية.

(ب) إن معدات وأساليب (ECCM) لا تحتاج إلى أقسام خاصة بل هو نشاط عام يستخدمه على سبيل المثال كل شخص يستخدم أجهزة الإتصالات، إلا من ناحية إعداد تلك الأساليب والمواصفات للمعدات.

(جـ) لكل قوة جوية كانت أو برية أو بحرية إحتياجاتها الخاصة بها لتحقيق أهداف الحرب الإلكترونية وذلك طبقا لطبيعة عملها ومعداتها ومواصفاتها فنحتاج إلى تنظيم داخلي قد يكون مخالف في بعض الشيء عن أقسام الحرب الإلكترونية في القوات الأخرى.

(د) يجب وضع قنوات ربط وتنسيق فيما بين أقسام الحرب الإلكترونية في القوات الثلاث وذلك بوضع قسم مركزي يحقق ذلك الربط والتنسيق.

(هـ) إدخال تنظيم الحرب الإلكترونية ضمن تنظيمات مراكز العمليات المختلفة.

(٢) فإذا ما أخذت تلك الأمور بعين الإعتبار عند إعداد التنظيم وإنشاء الحرب الإلكترونية تحققت بذلك النتائج المرجوة من:

أ ـ جمع المعلومات والإستفادة منها بأقل جهد ومعدات ممكنة.

ب ـ سهولة تبادل المعلومات والخبرات وتداولها بين أقسام الحرب الإلكترونية المختلفة.

جـ ـ التخلص من التداخل والتأثيرالسلبي على المعدات والأسلحة المختلفة، وتحقيق التناسق (الإنسجام) الكهرومغناطيسي (ELECTROMAGNETIC COMPATIBIL-ITY- (EMC)).

(٢) مستويات أنشطة الحرب الإلكترونية:

(أ) المستوى القيادي : وهو القسم المتواجد في رئاسة الأركان العامة أو في وزارة الدفاع والذي يضع السياسات العليا والأهداف العامة والتخطيط ووضع الاحتياجات المستقبلية في مجال الحرب الإلكترونية للقوات الثلاث.

(ب) المستوى التعبوي : وهو القسم المتواجد في قيادة القوة الجوية أو البرية أو البحرية والذي يضع التخطيط والتعليمات والتدريبات المناسبة لتنفيذ عمليات الحرب الإلكترونية.

(ج) المستوى التنفيذي : وهي الأقسام التي تقوم فعليا بعمليات الحرب الإلكترونية من مراقبة وتشويش وحماية إلكترونية ضمن العمليات الحربية.

٤ ـ تعليمات الحرب الإلكترونية (E. W. S.O.P):

ويقصد بها التعليمات الواجب تنفيذها والتقيد بها من قبل مستخدمي أجهزة ومعدات الإرسال والإستقبال، وهي إما أن تكون تعليمات عامة، تخص جميع الرادارات على سبيل المثال، وإما أن تكون تعليمات تخص رادار أو جهاز معين.

(١) إن من مهام الحرب الإلكترونية الإيجابية إعاقة وشل وخداع رادارات وإتصالات ومعدات أسلحة العدو للحصول على النتائج التالية :

أ ــ رد فعل العدو الخاطىء.

ب ــ رد فعل العدو المتأخر.

وهذان الهدفان من شأنهما تقليل فعالية العمليات الحربية والتأثير السلبي على مجريات الأحداث ونتائج الحرب. لذا يجب التنبيه والإعداد لتجنب حدوث مثل هذه النتائج في قواتنا ولتحقيق ذلك يجب الإهتمام بتعليمات الحرب الإلكترونية الصادرة بذلك لتنفيذها والتدريب عليها ومراقبة نتائجها، حتى يتم اختبارها ومعرفة مدى فعاليتها وتأثيرها للوصول إلى تعليمات مناسبة وعملية .

(٢) الأمور التي يجب أن تتضمن في تعليمات الحرب الإلكترونية :

أ ــ عدم تمكين العدو من الإستفادة من موجاتنا الكهرومغناطيسية المنبعثة من أجهزة الإرسال الخاصة بنا والتي يستفيد منها في برمجة وإعداد أجهزته الخاصة بالتشويش.

ب ــ عدم تمكين العدو من تحقيق الإعاقة والمخادعة لمعدات الإرسال لدينا، وذلك باستخدام تعليمات عامة وتعليمات خاصة لمعدات معينة، لتحقيق رد فعل مناسب وسريع .

جـ ــ وضع التعليمات المناسبة لجمع المعلومات وبرمجة وإعداد أجهزة التشويش ضد العدو.

(٣) التعليمات الخاصة لمراكز العمليات. والتي تمكن مراكز العمليات من إصدار الأوامر المناسبة لتنفيذ رد فعل مناسب وسريع ضد أعمال العدو الإلكترونية المضادة وذلك تفاديا لأي تأخير أو خطأ ومن أمثلة ذلك:

أ ــ عند قيام العدو بالتصوير مثلا، يجب تغيير مواقع الأسلحة والتأهب لرد الفعل

السريع.

ب ـ عدم تشغيل أجهزة الإرسال المهمة في معدات الأسلحة عند قيام العدو بعمليات استفزاز متعمدة.

جـ ـ عند التأكد من اتباعه أسلوب الحماية الإلكترونية اختيار البدائل بشكل سريع.

هذا ويجب التنبيه إلى أن تعليمات الحرب الإلكترونية يجب أن تتناسب مع حالات الإستعداد المختلفة في القوات المسلحة.

الباب السادس

أهداف الحرب الالكترونية

مما تقدم نستطيع بلورة أهداف الحرب الإلكترونية في ثلاثة أهداف رئيسية وهي :

١ ـ تقدير قوة العدو وتسليحه وتشكيلات جيشه، وتحديد مواقعه ومعرفة بعض أسراره العسكرية، وذلك من خلال الإستطلاع والإستفادة من معلوماته المرسلة ومراقبتها وتحليلها (الإجراءات الإلكترونية المساندة (ESM) وإستخبارات الإشارة).
ومن ثم نحدد موقفنا منه عسكريا وسياسيا واقتصاديا. كما نستطيع أن نكوّن تصورا أوضح عن مستقبل علاقاتنا معه.

٢ ـ التقليل من فعاليات أسلحة العدو وأجهزته على إختلاف أنواعها، وذلك بالتأثير عليها باستخدام أجهزة (ECM) (الإجراءات الإلكترونية المضادة)، لتكون النتيجة لصالحنا دفاعيا وهجوميا.

٣ ـ رفع كفاءة عملياتنا العسكرية المعتمدة على الأجهزة والمعدات الإلكترونية، وذلك بحماية تلك الأجهزة والمعدات (باستخدام المضادات الإلكترونية للإجراءات المضادة (ECCM) من تأثير العدو عليها باستخدامه الإجراءات الإلكترونية المضادة (ECM)، ومن استفادته من موجاتنا الكهرومغناطيسية الفعالة باستخدام الإجراءات الإلكترونية المساندة (ESM).

لكن كل هذا لا يكتمل بدون التخطيط السليم وتحديد الأهداف الحالية والمستقبلية بصورة واضحة حتى تكوّن بالتالي نتيجة التخطيط سليمة وصحيحة.

وسنذكر بعض النقاط المهمة المتعلقة بالحرب الإلكترونية :

١ ـ يجب أن يكون هناك تخطيط واع وواضح ودقيق عند الشروع أو التفكير في شراء أجهزة الحرب الإلكترونية، إذ أنه حتى في مجرد الشراء فإن بعض الحالات تجلب الضرر من حيث أريد بها المنفعة، فيجب ـ مثلا ـ مراعاة أن تكون أجهزة الحرب الإلكترونية المشتراة ملائمة لإمكانات القوات المسلحة وكفاءتها.

وبما أن لهذه الأجهزة علاقة ـ ولو بصورة غير مباشرة ـ بالأعداء فيجب أن تكون مزودة بإمكانات تستطيع باستخدامها الإستفادة والتأثير والحماية من أجهزة العدو كما وكيفا .

٢ ــ كما يجب أن تكون جميع أساليب الحرب الإلكترونية ـ والتي ذكرنا بعضا منها ـ مفهومة ومدروسة من قبل العسكريين وخاصة الذين يتعاملون مع الأجهزة ويجب كذلك أن تضع الحكومة لنفسها خطة مستقبلية، حتى إذا حدث وشوشت دولة ما على الإتصالات أو الرادارات مثلا، فإننا نكون على أهبة الاستعداد تحسبا لما يعقب التشويش، خاصة وأن التشويش يحدث عادة قبيل الهجوم المسلح .

٣ ــ يجب العمل كذلك بقاعدة (EMC « ELECTRO-MAGNETIC COMPATIBILITY) وهي الأساليب التي من شأنها ـ إذا اتبعناها ـ أن تمنع أجهزتنا المستخدمة في بعض مواقعنا من التأثير على بقية الأجهزة في المواقع الأخرى، أي أنها تقوم بمهمة الوقاية والحماية من التداخل غير المقصود (ACCDENTIAL INTERFERENCE) وإلا فإن الأجهزة أو الأسلحة التي نستخدمها تكون سلاحا ذا حدين . ولا يقتصر هذا على أجهزة الحرب الإلكترونية ، بل ينسحب على جميع الأجهزة والأسلحة الأخرى . إذ حدث في حرب ١٩٧٣ أن أسقطت أعداد من الطائرات بأسلحة صديقة(١) كما حدث تشويش على بعض الأجهزة من قبل أجهزة تشويش صديقة أيضا .

٤ ــ ألا نغفل جانب التدريب لما له من أهمية قصوى، إذا بالتدريب الجاد والمستمر يدرك الأفراد الأجهزة التي يتعاملون معها، فيكون إستخدامهم إياها إستخداماً مثالياً يؤدي إلى تحقيق الأهداف تحقيقاً كاملاً .

وهناك ما هو أهم مما تقدم وهو أن يكون في يقين القارىء أن ما قدمناه هو جزء من عدة الحرب التي أمرنا كمسلمين أن نعدها لعدو الله وعدونا على أن النصر من عند الله فقط ولا محل لإختلاق أسباب النصر إن لم نكن مع الله ولله .

﴿ إنما النصر من عندالله ﴾ ، ﴿ إن تنصروا الله ينصركم ويثبت أقدامكم ﴾ صدق الله العظيم .

وآخر دعوانا أن الحمد لله رب العالمين .

---

(١) مجلة INTERNATIONAL DEFENCE REVIEW عدد خاص عن ELECTRONIC WARFARE سنة ١٩٧٨ صفحة ٧.

مصطلحات الحرب الإلكترونية

E. W. GLOSSERY

No.	ABBR.	STANDS FOR	المعنى
1.	A.A.A	ANTI-AIRCRAFT ARTILIARY	المدافع المضادة للطائرات وهي مدافع أرضية مضادة للطائرات .
2.	A.A.M	AIR-TO-AIR MISSILE	صواريخ جو - جو صاروخ ينطلق من الطائرات ضد الطائرات .
3.	A/C	AIRCRAFT	طائرة
4.		ACCIDENTAL JAMMING	التشويش المصادف ، وهو تشويش يحدث على أجهزة صديقة بطريقة الصدفة وليس عن عمد (العرضي)
5.		ACCEDENTAL INTERFERENCE	التداخل غير المقصود (العرضي) المصادف
6.		ACTIVE MISSILE	الصاروخ الإيجابي ، وهو نوع من الصواريخ يتوجه نحو الأهداف المعادية عن طريق رادار موجود في الصاروخ يرسل نبضات تصطدم في الهدف فيستقبل الصاروخ صداها ثم يحدد إتجاه الهدف وبعده ثم يتوجه إليه . (مزود بجهاز ارسال واستقبال) .
7.	AD	AIR DEFENCE	الدفاع الجوي
8.	A.F.	AUDIO FREQUENCY	الذبذبات أو الترددات المسموعة (وهي لجميع الأصوات التي يستطيع الإنسان سماعها بأذنيه) وهي عادة من ٢٠ هرتز إلى ٢٠ كيلو هرتز.
9.	ADA	AIR DEFENCE ALERT	حالة استعداد تام للتصدي لطائرات العدو
10.	AECM	ACTIVE ELECTRONIC COUNTER MEASURES	الاجراءات الالكترونية المضادة الايجابية .

NO.	ABBR.	STANDS FOR	المعنى
11.	AEW	AIRBORNE EARLY WARNING	الانذار المبكر الجوي هو عملية تنبيه مبكرة عن الأهداف المعادية، وخاصة البعيدة، والمنخفضة منها وتقوم بها طائرات مثل طائرة الأواكس الأمريكية مستخدمة في ذلك أجهزة خاصة وبالذات الرادار البعيد المدى.
12.	AM	AMPLITUDE MODULATION	تضمين أو تعديل الإتساع وهي واحدة من طرق حمل المعلومات المراد إرسالها بالراديو أو الرادار على الذبذبات الناقلة FC.
13.		ANTI-ESM	المضادات الإلكترونية للإجراءات الإلكترونية المساندة.
14.		ANTI-ECM	المضادات الإلكترونية للإجراءات الإلكترونية المضادة
15.		ANTENNA	الهوائي، وهو الجزء الذي يرسل الجهاز عن طريقه طاقته وموجاته الكهرومغناطيسية ويستقبلها.
16.	ANTI-ARM	ANTI-ANTIRADIATION MISSILE	صاروخ موجه مضاد للصواريخ المضادة لأجهزة الإرسال.
17.	A.J.	ANTI-JAMMING	مضادات التشويش
18.	A.R.M.	ANTIRADIATION MISSILE	صاروخ موجه ضد أجهزة الإرسال (خاصة ضد الرادارات الأرضية).
19.	ATGM	ANTI-TANK GULDED MISSILE	صاروخ موجه مضاد للدبابات.
20.	AWACS	AIRBORNE WARNING AND CONTROL SYSTEM	نظام الانذار والتحكم الجوي، وكلمة أواكس عادة تطلق على الطائرة الأمريكية البوينغ ٧٠٧ E-3A للانذار المبكر.
21.	ASPJ	AIRBORNE SELF-PROTECTION JAMMER	جهاز تشويش (للحماية الذاتية) تطلق هذه التسمية على أجهزة التشويش المحمولة على الطائرات وتكون عادة أوتوماتيكية الحركة أي حالما يجد الجهاز أنه مراقب من رادار معادي كشفي يقوم بكشف مركز «LOCK-ON» فإنه يشوش عليها.
22.	ATC	AIR TRAFFIC CONTROL	التحكم أو مراقبة الحركة الجوية
23.		BLANKETING	إشارة أو ذبذبة ذات طاقة عالية تتداخل في شبكة اتصالات (تشويش فعال).

NO.	ABBR.	STANDS FOR	المعنى
24.	BTY	BATTERY	بطارية دفاع جوي (موقع للصواريخ المضادة للطائرات)
25.		BURNTHROUGH	الاحتراق المخترق، وهي عملية زيادة طاقة الإرسال الراداري للتخلص أو التقليل من تأثير التشويش على الردار، فتكون إشارة إرسال الرادار أعلى من إشارة التشويش.
26	BW	BANDWIDTH	عرض المجال
27.	BW	BEAM WIDTH	عرض الشعاع
28.	C^2	COMMAND AND CONTROL	القيادة والسيطرة
29.	C^3	COMMAND, CONTROL AND COMMUNICATIONS	القيادة والسيطرة والإتصالات
30.	C^3I	COMMAND, CONTROL, COMMUNICATION AND INTELLIGENCE	القيادة والسيطرة الإتصالات باستخدام وسائل الاستخبارات المختلفة وخاصة الاستخبارات الإلكترونية.
31.	CIO	COMBAT INTELLIGENCE OFFICER	ضابط استخبارات حربي
32		CLUTTER	هي كل الأهداف (أو الأشياء غير المرغوب فيها) التي تظهر على شاشة الرادار مثل المؤثرات الناتجة عن حالات الطقس، المباني، . . الخ .
33.	COMM.	COMMUNICATION	الاتصال « أجهزة الإتصالات »
34.	CM	COUNTERMEASURES	الاجراءات المضادة
35.	COMINT.	COMMUNICATION INTELLIGENCE	استخبارات الإتصالات
36.	COMSEC.	COMMUNICATION SECURITY	أمن الاتصالات، وهي جميع الأشياء التي تكفل أمن وحماية الاتصالات من أساليب فنية وأجهزة تشفير. . . الخ.
37.		CROSS-EYE-JAMMING	وهي إحدى طرق التشويش « خاصة بالرادار » تتم عن طريق جهازين من أجهزة التشويش يوضعان في أماكن مختلفة ويكون إرسالها « أشعتها » متقاطعا قبيل الرادار المراد التشويش عليه، لتعميته عن معرفة مصدر التشويش.

NO.	ABBR.	STANDS FOR	المعنى
38.	C/S	CYCLE PER SECOND	. . . . موجات/الثانية، مقياس الذبذبات أو الترددات وهي نفس الهرتز. (انظر HERTZ)
39.	C.W.	CONTINOUS WAVE	الموجات المستمرة، وهو نوع من إرسال الرادار
40.	C.W.J.	CONTINOUS WAVE JAMMING	جهاز تشويش ذو إشارة « مستمرة الموجات » على أجهزة العدو.
41.	D.E.CM	DEFENSIVE ELECTRONIC COUNTERMEASURES	الاجراءات الإلكترونية المضادة الدفاعية أي المستخدمة للعمليات الدفاعية فقط.
42.	D.E.CM	DECEPTIVE ELECTRONIC COUNTERMEASSURES	الاجراءات الإلكترونية المضادة المخادعة
43.	D.F.	DIRECTION FINDER	موجد الإتجاه، وهو جهاز مهمته تحديد اتجاه الأجهزة المرسلة.
44.		DECOY	الطعم، وهو عادة طائرة صغيرة لها نفس خواص الهدف المثالي للرادارات فتظهر على الشاشة وكأنها هدف كبير لتحجب الهدف الحقيقي، وقد تكون مزودة بأجهزة إلكترونية.
45.		DRONE	الطائرة التي تطير بدون طيار، ويتحكم بطيرانها عن بعد بجهاز التحكم عن بعد: REMOTE CONTROL أو التي تطير طيرانا مبرمجاً.
46.	EC[4]	ELECRTONIC COMMAND CONTROL, COMMUNICATION AND COUNTERMEASURES	«القيادة والسيطرة والإتصالات والإجراءات المضادة » الإلكترونية : وهي (C^3) معتمدة على استخدامات الاجراءات الإلكترونية المضادة .
47.	E.H.F.	EXTREMELY HIGH FREQ.	الذبذبات المتناهية العلو، وهي التي تتراوح بين : ٣٠ ڤيقا هرتز و ٣٠٠ ڤيقا هرتز .
48.	ECM	ELECTRONIC COUNTERMEA-SURES	الاجراءات الالكترونية المضادة
49.	ECCM	ELECTRONIC COUNTER-COUNTERMEASURES	المضادات الإلكترونية للاجراءات المضادة
50.	EMI	ELECTRO-MAGNATIC IN-TERFERENCE	التداخلات الكهرومغناطيسية
51.	E.O.B.	ELECTRONIC ORDER OF BATTLE	الموقف الألكتروني للمعركة

NO.	ABBR.	STANDS FOR	المعنى
52.	ELSEC	ELECTRONIC SECURITY	الأمن الالكتروني، أو الحماية الالكترونية
53.		ELECTRONIC DECEPTION	التضليل أو الخداع الإلكتروني .
54.	ELINT	ELECTRONIC INTELLIGENCE	الاستخبارات الالكترونية
55.	EMP	ELECTRO-MAGNETIC PULSE	النبضة الكهرومغناطيسية، وهي نبضة كهربائية مغناطيسية تكون حادة وسريعة جدا وعالية الطاقة .
56.		ECHOES	انعكاس الاشارات (الاصداء)
57.	EMC	ELECTRO-MAGNETIC COM-PATIBILITY	الانسجام الكهرومغناطيسي: وهو أسلوب من شأنه أن يجعل أجهزتنا عند استخدامها عديمة التأثير أو التشويش على الأجهزة الصديقة
58.	E.R.	ELECTRONIC RECONNASS-ANCE	الاستطلاع الالكتروني: أي الاستطلاع باستخدام الأجهزة الالكترونية من كشف ومراقبة ذبذبات الراديو وذبذبات الرادار والتصوير.. الخ
59.	ERASE	ELECTRO-MAGNETIC RADIA-TION SOURCE ELIMINATION	عملية تدمير مصادر الاشعاع الكهرومغناطيسي
60.	ESM	ELECTRONIC SUPPORT MEA-SURES (OR ELECTRONIC WARFARE SUPPORT MEA-SURES)	الاجراءات الالكترونية المساندة
61.	EW	ELECTRONIC WARFARE	الحرب الالكترونية
62.		EARLY WARNING	التحذير أو الانذار المبكر وهو عملية تنبيه مبكر عن الأهداف المعادية تقوم بها أجهزة معينة، وخاصة الرادار البعيد المدى.
63.	EWO	ELECTRONIC WARFARE OFFICER	ضابط الحرب الإلكترونية . وهذه التسمية معروفة في معظم جيوش الدول المتقدمة .
64.	EX.JAM.	EXPENDABLE JAMMER	أجهزة التشويش المقذوفة، وهي من الاجراءات الالكترونية المضادة .
65.	F.	FIGHTER	طائرة عسكرية مقاتلة

NO.	ABBR.	STANDS FOR	المعنى
66.		FOLLOWER JAMMER	جهاز تشويش ملاحق، وهو جهاز عندما يستقبل ذبذبات العدو يقوم بالتشويش عليها فإذا انتقلت ذبذبة العدو إلى ذبذبة أخرى تبعها وشوش عليها وهكذا (خاص بالاتصالات)
67.		FERRETE	وهي طائرة أو سفينة أو آلية عسكرية تحمل أجهزة SIGINT و ESM وتحلق قرب مواقع العدو مبتعدة عن نطاق أو مجال دفاعه الجوي وراداراته وصواريخه لكشف ومراقبة وتحديد مواقع جميع أجهزة الإرسال المعادية.
68.		FREQUENCY HOPPING	تنقل التردد: وهو عملية إرسال الذبذبة أو التردد الحامل FREQUENCY CARRIER ١٠٠٠ نقلة (HOP) في الثانية ويكون ذلك في مجال ٦ أو ٣٠ميغا هرتز أو أقل أو أكثر.
69.		FIRE FINDER	نظام دقيق وسريع لتحديد مصادر اطلاق النار الأرضية المعادية.
70.		FREQUENCY AGILITY	تنقل الذبذبات، تنتقل ذبذبات الإرسال من ذبذبة إلى أخرى بسرعات متفاوتة حسب تصميم الجهاز وتكون حوالي بضع عشرة ذبذبة في مجال عريض، وهذه العملية تتم في الرادار عادة للتغلب على التشويش والمراقبة .
71.		FREQUENCY DIVERSITY	تنوع الذبذبات، وهو أن يكون هناك رادارا له أكثر من ذبذبة يستخدمها في نفس الوقت أو على فترات قصيرة جدا ويكون بين الذبذبة والأخرى مجال عريض، وهذا من شأنه التخلص أو التقليل من تأثير التشويش.
72.	FM	FREQUENCY MODULATION	تعديل التردد أو تضمين التردد، وهي إحدى طرق حمل المعلومات المراد إرسالها بالراديو أو الرادار على الذبذبات الناقلة « F_C »
73.	G.C.A.	GROUND CONTROLLED APROACH	وهو رادار أرضي، مهمته التحكم والسيطرة على الأهداف القريبة من موقعه كالطائرات المقلعة والهابطة في القواعد الجوية والمطارات (لهبوط الطائرات راداريا)

NO.	ABBR.	STANDS FOR	المعنى
74.	G.C.I.	GROUND CONTROLLED INTERCEPTION	وهو رادار للسيطرة وتوجيه الطائرات المقاتلة الصديقة ضد الطائرات العسكرية المعادية.
75.	GEOREF	GEOGRAPHICAL REFERENCE	الاحداثيات الجغرافية
76.	GHZ	GIGAHEART	اصطلاح يعني: ألف مليون (مليار) هرتز (مليار موجة في الثانية).
77.	H.	HOSTILE	عدو
78.		HOPPING FREQUENCY	التردد المتنقل، وهو تنقل التردد في الثانية. (عدد النقلات في الثانية).
79.	HARM	HIGH SPEED ANTI-RADIATION MISSILE	صواريخ سريعة مضادة لأجهزة إرسال العدو.
80.	H.F.	HIGH FREQUENCY	الذبذبات العالية وهي من ٣ ميغا هرتز إلى ٣٠ ميغا هرتز
81.	H.F.R.	HIGHT FINDER RADAR	رادار موجد ارتفاع الأهداف عن سطح الأرض أو البحر .
82.	HOJ	HOME-ON-JAM	التوجيه نحو التشويش، وهي عملية تتم بإستخدام الأجهزة الإلكترونية أو الصواريخ الموجة السلبية ، لمتابعة وملاحقة اتجاه مصدر التشويش. (خاص بالصواريخ).
83.	HZ.	HERTZ	مصطلح يعني عدد الذبذبات في الثانية، وحدة قياس التردد والذبذبة.
84.		INTENTIONAL INTERFERENCE	التداخل المقصود، وهو باختصار التشويش المعادي بأنواعه.
85.		INTERNAL INTERFERENCE	التداخل الداخلي، وهو حدوث خلل داخل الجهاز الالكتروني نتيجة وجود عطل حقيقي فيه يؤثر على أدائه.
86.		INTERFERENCE	التداخل، وهو أية اشارة غير مرغوب فيها تدخل في الأجهزة أو الدوائر الكهربائية والالكترونية، وهذه الإشارة إما أن تكون إشارة كهرومغناطيسية (ELECTRO-MAGNETIC) تتداخل في الجهاز آتية عبر الأثير أو تكون إشارة كهربائية (ELECTRICAL) تتداخل في الجهاز آتية عبر الأسلاك الكهربائية.

NO.	ABBR.	STANDS FOR	المعنى
			وهذا التداخل يؤثر على الأجهزة أو التشويش عليها فيقلل من فعاليتها ويتفاوت هذا التأثير بتفاوت قوة الإشارة المتداخلة ، ومن التداخل : ١ ـ التداخل المقصود INTENTIONAL INTERFERANCE ٢ ـ التداخل غير المقصود (العرضي) ACCEDENTAL INTERFERANCE ٣ ـ التداخل الطبيعي NUTURAL INTERFERANCE ٤ ـ التداخل الداخلي : INTERNAL INTERFERANCE
87.	IFF	IDENTIFICATION FRIEND OR FOE	التمييز بين الصديق والعدو ويتم ذلك عن طريق جهاز راداري SSR (SECONDARY SURVILL-ANCE RADAR) يرسل نبضتين إلى الأهداف على هيئة سؤال فإن كان الهدف صديقا أجاب بإرسال رموزأو شفرة مطابقة ومتفق عليها، أما إذا لم يرسل مطلقا أو كانت شفرته ورموزه مختلفة فإنه يعتبر هدفا معاديا .
88.		INTERCEPT RECEIVER	جهاز استقبال دقيق لرصد وكشف خواص ذبذبات العدو المنبعثة من أجهزة الارسال ولمعرفة المعلومات المرسلة .
89.	I.R.	INFRA RED	الأشعة تحت الحمراء وهي تتراوح تقريبا بين : ١٠٦ ميغا هرتز و١٠^٨ ميغا هرتز
90.	I.R.CM.	INFRA RED COUNTERMEA-SURES	الاجراءات الالكترونية المضادة المستخدمة ضد الأجهزة التي تستخدم الأشعة تحت الحمراء (خاصة ضد الصواريخ الموجهة المستخدمة تلك الأشعة) .
91.	I.R.W.R.	INFRA RED WARNING RE-CEIVER	جهاز استقبال يكشف وينذر عن وجود هدف معاد تنبعث منه أشعة تحت الحمراء .
92.	I.R.G.M.	INFRA RED GUIDED MISSILE	نوع من الصواريخ تتبع المصادر التي تنبعث منها الأشعة تحت الحمراء (وهي صواريخ سلبية انظر PASSIVE MISSILE)

NO.	ABBR.	STANDS FOR	المعنى
93.	I.S.B.	INDEPENDANT SIDE BAND	المجال الجانبي المستقل (خاص بالاتصالات) .
94.	I.R.CCM.	INFRA RED COUNTER COUN-TERMEASURES	وهو جهاز أو أسلوب يستخدمه الجهاز أو الصاروخ الذي يرصد الأشعة تحت الحمراء ، للتخلص أو التقليل من تأثير التشويش على الجهاز أو الصاروخ.
95.	IPAR	IMPROVED PULSE AQUISI-TION RADAR	رادار معدل نبضي الكشف
96.	ID	IDENTIFICATION	التمييز (تمييز الأشخاص والارساليات والأهداف الصديقة من المعادية) .
97.	JAFF	EXPRESSION FOR THE COM-BINATIONS OF ELECTRONIC AND CHAFF JAMMING	« وهو إستخدام أجهزة التشويش الإيجابية والنصلات للتشويش » .
98.	J.O.C	JOINT OPERATONS CNETER	مركز العمليات المشتركة
99.	JTIDS	JOINT TACTICAL INFORMA-TION DISTRIBUTION SYSTEM	وهذا نظام اتصالات متطور لارسال واستقبال عدة معلومات لعدة أجهزة استقبال وإرسال في آن واحد (وهو نفس نوع الأجهزة المستخدمة في طائرات الأواكس الأمريكية) .
100.	J/S R	JAMMING TO SIGNAL RATIO	نسبة طاقة إشارة التشويش إلى طاقة إشارة الذبذبة المستعملة .
101.	K.Hz.	KILO HERTZ	كيلو هرتز (ألف موجة في الثانية)
102	LASER	LIGHT AMPLIFICATION BY STIMULATED EMISSION OF RADIATION	اشعاع الليزر: وهي تعني: تكبير الضوء بطريقة الانبعاث المتحدد للاشعاع .
103.	LF	LOW FREQUENCY	الذبذبات المنخفضة وهي التي من: ٣٠ كيلوهرتز إلى ٣٠٠ كيلو هرتز
104.	LSB	LOWER SIDE BAND	المجال الجانبي السفلي (خاص بالإتصالات) .
105.	LWR	LASER WARNING RECEIVER	جهاز استقبال يكشف وينذر عن وجود هدف معاد يستخدم أشعة الليزر
106.		MEASURES	الاجراءات أو التدابير
107.	MF	MEDIUM FREQUENCY	الذبذبات المتوسطة وهي التي من ٣٠٠ كيلو هرتز إلى ٣ ميغاهرتز.

NO.	ABBR.	STANDS FOR	المعنى
108.	MHZ	MIGA HERTZ	مليون هرتز (مليون موجة في الثانية) .
109	MOD	MODULATION	التضمين، وهي عملية وضع المعلومات المراد إرسالها على التردد أو الذبذبة الحاملة .
110.	MTI	MOVING TRAGET INDICATION	اظهار الهدف المتحرك، وهذا من خواص شاشة الرادار التي تظهر عليها الأهداف المتحركة فقط كالطائرات، وليس الأهداف الثابتة من جبال ومبان وغيرها .
111.		MUSIC	اصطلاح يطلق عند حدوث تشويش الكتروني منبعث من أجهزة العدو.
112.	NAEW	NATO AIRBORNE EARLY WARNING	الانذار المبكر الجوي لحلف الناتو.
113		NATURAL INTERFERENCE	التداخل الطبيعي، وهو تأثير العوامل الطبيعية في أجهزة الاستقبال الالكترونية (من اتصال ورادار) ويقلل من فعالية تلك الأجهزة.
114.	NAV	NAVIGATION	(الأجهزة الملاحية) .
115.	NAVAID	NAVIGATION AID	الأجهزة الملاحية المساندة، وهي جميع الأجهزة الملاحية المساعدة للطائرات والسفن. . الخ .
116.	NEMP	NUCLEAR ELECTROMAGNA-TIC PULSE	النبضة الكهرومغناطيسية النووية، وهي نبضة حادة وسريعة وذات طاقة عالية جدا تحدث عند انفجار القنابل النووية، وإذا وصلت إلى أي جهاز كهربائي أو الكتروني تعطله عن العمل.
117.		NOISE	الضجيج والضوضاء ، الاشارات غير المرغوب فيها بالأجهزة الكهربائية أو الالكترونية ، ولها أنواع كثيرة منها ما هو طبيعي ومنها ما هو من الأجهزة الكهربائية والالكترونية نفسها ، ويكون صوت الضوضاء كصوت محرك السيارة أو الطائرة مثلاً .
118.	NUDET	NUCLEAR DETONATION RE-PORT	تقرير انفجار ذري
119.		OFF-LINE-JAMMING	جهاز يقوم بالتشويش في غير اتجاه الهدف والرادار المراد التشويش عليه، ويمكن أن يكون من

NO.	ABBR.	STANDS FOR	المعنى
			الاجراءات الالكترونية المضادة الايجابية أو السلبية .
120.		ON-LINE-JAMMING	جهاز يقوم بالتشويش في نفس اتجاه الهدف والرادار المراد التشويش عليه .
121.	OR	OUT OF RANGE	خارج مدى الرادار
122.	PECM	PASSIVE ELECTRONIC COUNTER MEASURES	الاجراءات الالكترونية المضادة السلبية .
123.		POLIRIZATION DIVERSITY	تغيير قطبية الهوائي : أفقيا أو رأسيا أو دائريا للتخلص أو التقليل من تأثير التشويش .
124.	PM	PULSE MODULATION	تضمين النبضة ، وهي من طرق حمل المعلومات المراد إرسالها بالراديو أو الرادار مثلا ، على الذبذبات الناقلة (الحاملة) .
125		PASSIVE MISSILE	الصاروخ السلبي ، وهو نوع من الصواريخ يتوجه نحو الأهداف المعادية عن طريق استقبال الموجات والذبذبات والترددات المنبعثة منها كأجهزة إرسال (الرادارات) ، أو التوجه نحو ذبذبات الأشعة تحت الحمراء المنبعثة من محرك الطائرات . . الخ . إذا فالصاروخ السلبي هو الذي يحوي فقط أجهزة استقبال للتوجه نحو الأهداف ، وهو ضمن الأجهزة السلبية PASSIVE EQUIPMENTS مثل صواريخ سام - ٧ الروسي SAM-7 وستنجر الأمريكي (STINGER) المعتمدين على انبعاث الأشعة تحت الحمراء المنبعثة من محرك الطائرة ، وصواريخ SHRIKE الأمريكية المعتمدة على إرسال الرادارات الأرضية المعادية . ومن عيوب الأجهزة أو الصواريخ السلبية فقدان القدرة على المتابعة والملاحقة والتوجيه عند انقطاع إرسال الأهداف .
126.	PPI	PLAN POSITION INDICATOR	شاشة الرادار
127.		PHASE MODULATION	وهي من طرق حمل المعلومات المراد إرسالها بالراديو أو الرادارا ، على الذبذبات الناقلة (الحاملة)

NO.	ABBR.	STANDS FOR	المعنى
128.	PRF	PULSE REPITETION FREQUENCY	تردد نبضة الذبذبة (خاص بالرادار : الرادار يعمل على إرسال النبضة (PULSE) وزمن استقبال (INTERVAL) و (PRF) هو عدد النبضات في الثانية .
129.	PNVS	PILOT NIGHT VISION SYSTEM	نظام في الطائرة يستخدم للرؤية الليلية .
130		POLARIZATION	الاستقطاب، وهي بالنسبة لهوائي أجهزة الاتصال أو الرادار . . الخ إما أن يكون أفقي HORIZANTAL أو رأسي القطبية VERTICAL أو دائري القطبية **CIRCULAR**
131.	P.S.R.	PRIMARY SURVEILLANCE RADAR	رادار كشف ابتدائي ، وهو رادار يكشف الأهداف ويعطي بعدها واتجاهها .
132.		PHANTOM TRAGET	الهدف الشبح ، نوع من الأهداف يرى على شاشة الرادار، يصعب التكهن عن ماهيته، ويمكن أن يحدث نتيجة تشويش مخادع أو ظاهرة طبيعية تؤثر في الرادار أو خلل في جهاز الرادار.
133.		PULSE COMPRESSION	ضغط النبضة، تقنية تستغل في الرادار ترسل النبضة طويلة وتيستقبلها الرادار قصيرة مضغوطة لتبين الأهداف على شاشة الرادار محددة وواضحة .
134.	QRC	QUICK REACTION CABABILITY	الاستعداد أو القابلية السريعة في رد الفعل .
135.	RGC	RANGE GATE CAPTURE	أسر بوابة المجال . نوع من أنواع التشويش المخادع على الرادارات .
136.	RGS	RANGE GATE STEELING	سرقة بوابة المجال، نوع من أنواع التشويش المخادع على الرادارات .
137.	RF	RADIO FREQUENCY	ذبذبات الراديو (أو الموجات الكهرومغناطيسية عامة)
138.	RFI	RADIO FREQUENCY INTERFERENCE	تداخل في ذبذبات الراديو، من تشويش وخداع وظواهر طبيعية مثل البرق، أو من معدات كهربائية قريبة من الأجهزة . . الخ .

NO.	ABBR.	STANDS FOR	المعنى
139.	RHAW	RADAR HOMING AND WARNING	جهاز رادار يقوم بالكشف والانذار عن الأهداف المعادية ويحدد اتجاهها .
140.		RADIO SILENCE	صمت الراديو أو صمت الإتصال وهو قطع الاتصال بأجهزة الراديو وعادة يكون قبيل أو أثناء الحرب .
141.	RINT	RADIATION INTELLIGENCE	رصد الذبذبات والموجات المنبعثة من أجهزة ارسال العدو ومراقبتها وكشفها وتحديد مصدرها وتحليلها .
142.		RAID	غارة
143.	RECCE	RECONNASSIANCE	الاستطلاع
144.	RPV	REMOTLY PILOTED VEHICLE	الطائرات التي تطير بدون طيار، التي يتحكم بطيرانها وأجهزتها بجهاز التحكم عن بعد: REMOTE CONTROL
145.		REPEATER JAMMER	جهاز التشويش المعاد .
146.	RWR	RADAR WARNING RECEIVER	جهاز استقبال راداري للكشف والانذار عن الأهداف المعادية التي تنبعث منها موجات رادارية وهو جهاز سلبي PASSIVE EQUIPMENT
147.	RADAR	RADIO DETECTION AND RANGING	وهو جهاز لكشف الأهداف المعادية ويحدد اتجاهها أو بعدها أو ارتفاعها أو يحدد هذه الأشياء جميعها .
148.	SAM	SURFACE-TO-AIR MISSILE	الصواريخ التي تنطلق من الأراضي أو البحر إلى الجو وهي صواريخ مضادة للأهداف الجوية .
149.	SHF	SUPER HIGH FREQUENCY	الذبذبات فوق المرتفعة وهي التي تتراوح بين ٣ جيجا هرتز إلى ٣٠ جيجا هرتز.
150.	S/J R	SIGNAL TO JAM RATIO	نسبة قيمة الإشارة الحقيقية إلى قيمة إشارة التشويش، وكلما علت هذه النسبة كان التشويش غير مؤثر .
151.	SLAR	SIDE LOOKING AIRBORNE RADAR	نوع من الرادارات يحمل على الطائرات للتصوير الجانبي الراداري (RADAR IMAGE) على مواقع العدو.
152.	SLB	SIDE LOBE BLANKING	جهاز لالغاء ظهور الأهداف المكتشفة عن طريق الأشعة الجانبية وعادة تستخدم للتخلص من التشويش على تلك الأشعة .

NO.	ABBR.	STANDS FOR	المعنى
153.	SLC	SIDE LOBE CANCELLER	جهاز يلغي ظهور الأهداف المكتشفة عن طريق الأشعة الجانبية وعادة تستخدم للتخلص من التشويش على تلك الأشعة (خاص بالرادار).
154.	S.L.J	SIDE LOBE JAMMING	التشويش الموجه نحو الأشعة الجانبية (خاص بالرادار)
155.	S.P.J	SELF-PROTECTION JAMMER	جهاز تشويش للحماية الذاتية عند حدوث متابعة من رادار العدو: RADAR LOCK-ON
156.		SEARCH RECEIVER	انظر (INTERCEPT RECEIVER)
157.		SPOOF	مصطلح في الحرب الالكترونية يعني التضليل والخداع.
158.		SEMI-ACTIVE MISSILE	صاروخ نصف ايجابي، أو صاروخ شبه ايجابي وهو نوع من الصواريخ يتوجه نحو الأهداف المعادية عن طريق جهاز رادار موجود في مكان آخر يرسل نبضات نحو الأهداف المعادية فتستقبل هذه الصواريخ صدى نبضات الرادار فتحدد اتجاه الأهداف وبعدها ومن ثم تتوجه إليها. (صاروخ مزود بجهاز رادار استقبال فقط معتمد على جهاز رادار آخر للإرسال).
159.	SSB	SINGLE SIDE BAND	المجال الجانبي المنفرد أو الحزمة الجانبية المنفردة (خاص بالاتصالات).
160.	SIGINT	SIGNAL INTELLIGENCE	استخبارات الاشارة
161.	SIF	SELECTIVE IDENTIFICATION FEATURES	عملية SIF هي نفس عملية I.F.F. (انظر IFF) لكنه أيضا يستخدم للحصول على معلومات أكثر عن الأهداف (مثلا رقم الطائرة).
162.	SSR	SECONDARY SURVILLANCE RADAR	وهو رادار خاص لتحديد هوية الهدف إذا كان صديقا أو معاديا (انظر SIF & I.F.F.)
163.	S.O.J	STAND OFF JAMMER	عملية اجراء التشويش بعيدا عن مسرح العمليات الحربية، وخارج نطاق الرادار المراد التشويش عليه.

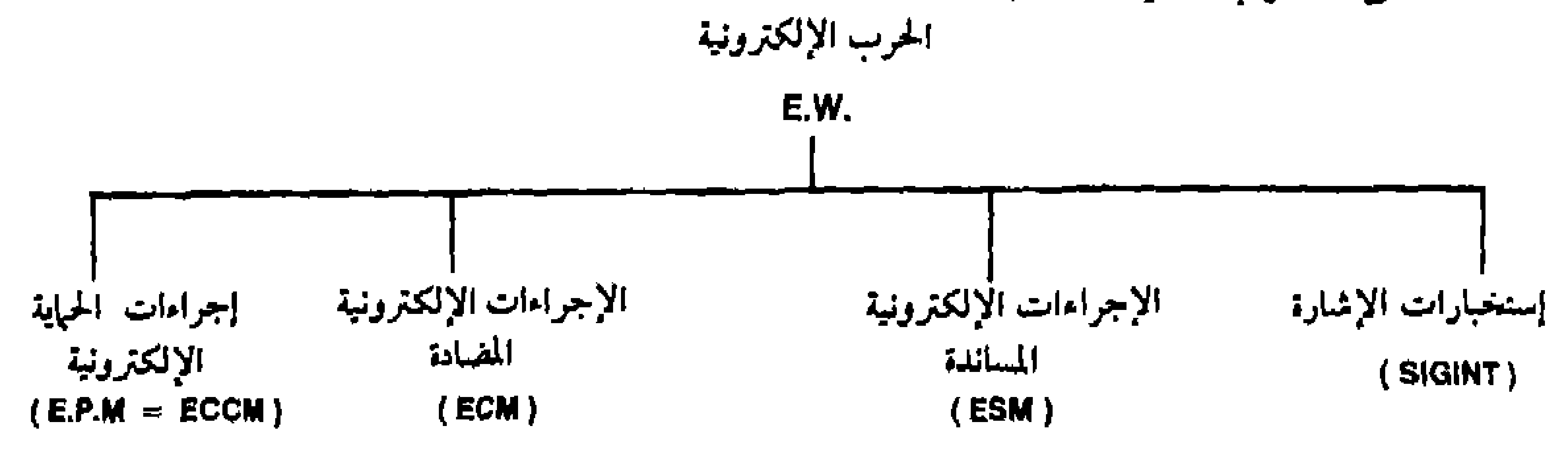
NO.	ABBR.	STANDS FOR	المعنى
164.	S.W.	SHORT WAVE	الموجات القصيرة وهي التي تراوح بين ٣ ميغا هرتز و٣٠ ميغاهرتز (مثل ذبذبات HF).
165.		SWEEPTHROUGH	جهاز يرسل تشوشا محددا على مجال عريض من الذبذبات عن طريق التشويش على ذبذبة بعد أخرى بسرعات مختلفة حتى يتم التشويش على المجال كله وهكذا تتكرر العملية مرارا .
166.		SCRAMBLE (A/C)	أمر الاقلاع الفوري للطائرة (للاعتراض)
167.		STANDBY	حالة استعداد
168.	TAC JAM	TACTICAL JAMMER	جهاز تشويش للعمليات التكتيكية أو ضد العمليات التكتيكية المعادية .
169.	TCJ	TACTICAL COMMUNICATION JAMMING	تشويش الاتصال التكتيكي .
170.	TD	TECTICAL DECISION	القرار التكتيكي .
171.	TEREC	TACTICAL ELECTRONIC RE-CONNAISSANCE SYSTEM	نظام الاستطلاع الالكتروني التكتيكي
172.		TERA HERTZ	تيرا هرتز =مليون ميغا هرتز .
173.	TEWS	TACTICAL ELECTRONIC WAR-FARE SYSTEM	نظام الحرب الالكترونية التكتيكي .
174.		TARGET SUSCEPTIBILITY	أن يكون الهدف عرضة للتأثير أو الاعطاب.
175.	TJS	TACTICAL JAMMING SYSTEM	نظام التشويش التكتيكي .
176.	TOJ	TRACK-ON-JAM	وهي عملية متابعة وملاحقة إتجاه إشارة التشويش المنبعثة من جهاز تشويش العدو (خاص بالرادار) .
177.		TARGET VULNERABILITY	أن يكون الهدف عرضة للتدمير أو السقوط بيد الأعداء .
178.	TWR	TAIL WARNING RADAR	وهو جهاز استقبال راداري يوضع في مؤخرة الطائرة يقوم بالانذار عن وجود رادار معاد متتبع للطائرة بهدف كشفها ، وهو مثل .R.W.R
179.	UHF	ULTRA HIGH FREQUENCY	الذبذبات فوق العالية وهي تتراوح بين ٣٠٠ ميغا هرتز و٣ جيجا هرتز.

NO.	ABBR.	STANDS FOR	المعنى
			والذبذبات فوق العالية العسكرية فهي التي من ٢٢٥ ميغا هرتز إلى ٤٠٠ ميغا هرتز (للإتصالات من الأرض إلى الجو أو العكس وأيضا الاتصالات جو - جو)
180.	USB	UPPER SIDE BAND	المجال الجانبي العلوي (خاص بالاتصالات).
181.	U.V.	ULTRA VIOLET	أشعة فوق البنفسجية وهي من ١٠^٩ ميغا هرتز إلى ١٠^١٢ ميغا هرتز
182.	VHF	VERY HIGH FREQUENCY	الذبذبات العالية جدا، وهي التي تتراوح بين ٣٠ ميغا هرتز و٣٠٠ ميغا هرتز والذبذبات العالية جدا العسكرية « للاتصالات جو - أرض وجو - جو) وهي من ١٠٠ ميغا هرتز إلى ١٦٣ ميغا هرتز.
183.	VLF	VERY LOW FREQUENCY	الذبذبات المنخفضة جدا وهي التي تتراوح بين ٣ كيلوهرتز و٣٠ كيلو هرتز.

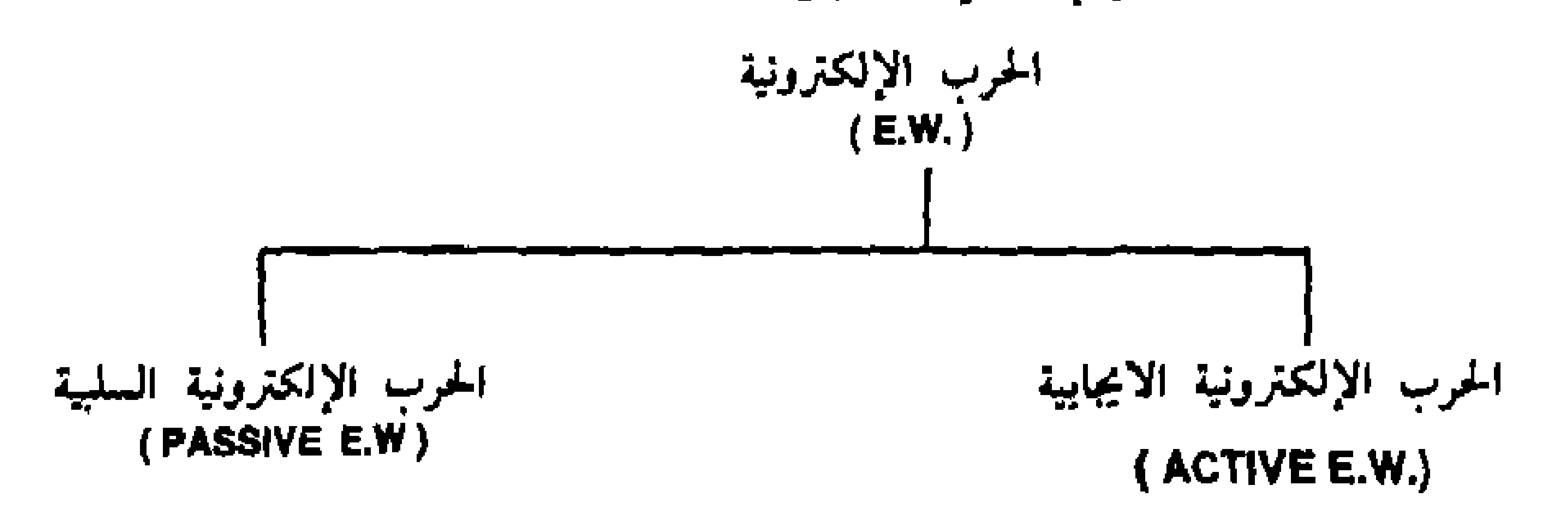
رسومات توضيحية مختصرة

سندرج هنا بعض الرسومات التوضيحية المختصرة هي زبدة الكتاب وقد تعين في التذكير وإسترجاع أسس الحرب الإلكترونية.

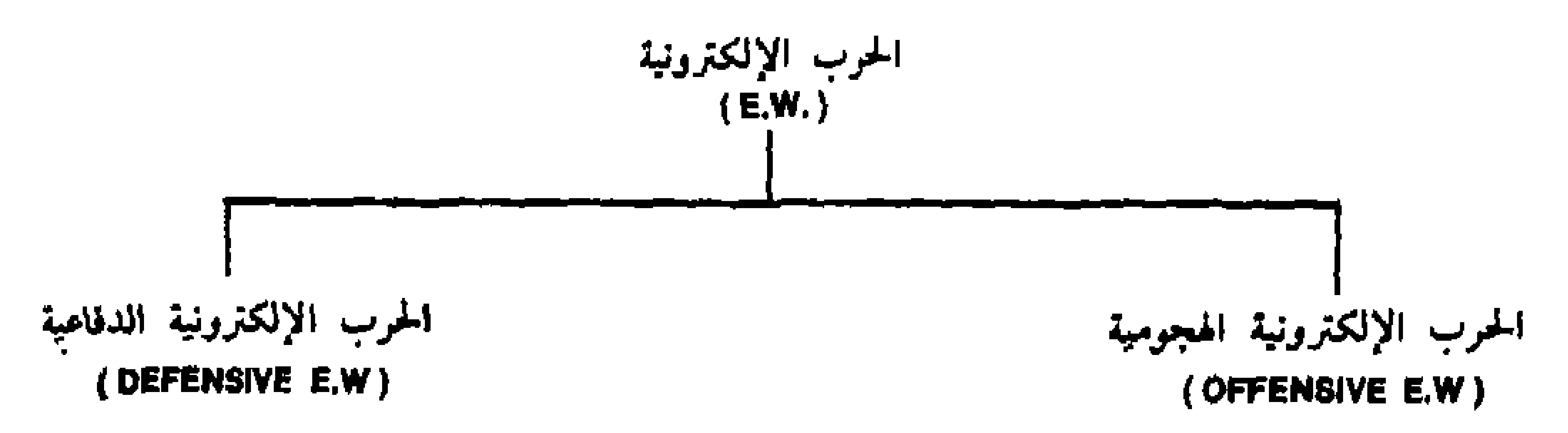
١ ـ أسس الحرب الإلكترونية



٢ ـ معدات وأجهزة الحرب الإلكترونية:



٣ ـ عمليات الحرب الإلكترونية :



٤ ـ نوعية معدات وأجهزة الحرب الإلكترونية :



٥ ـ أقسام إستخبارات الإشارة :

إستخبارات الإشارة
(SIGINT)

إستخبارات الإتصالات
(COMINT)

إستخبارات غير الإتصالات
(NONCOMM. INT)
(ELINT)

٦ ـ عمليات إستخبارات الإشارة :

إستخبارات الإشارة
(SIGINT)

إستخبارات الإشارة
الإستراتيجية
(STRATEGIC SIGINT)

إستخبارات الإشارة
التعبوية
(TACTICAL SIGINT)

٧ ـ معلومات (إستخبارات الإتصالات) :

إستخبارات الإتصالات
(COMINT)

الصوتية
(VOICE)

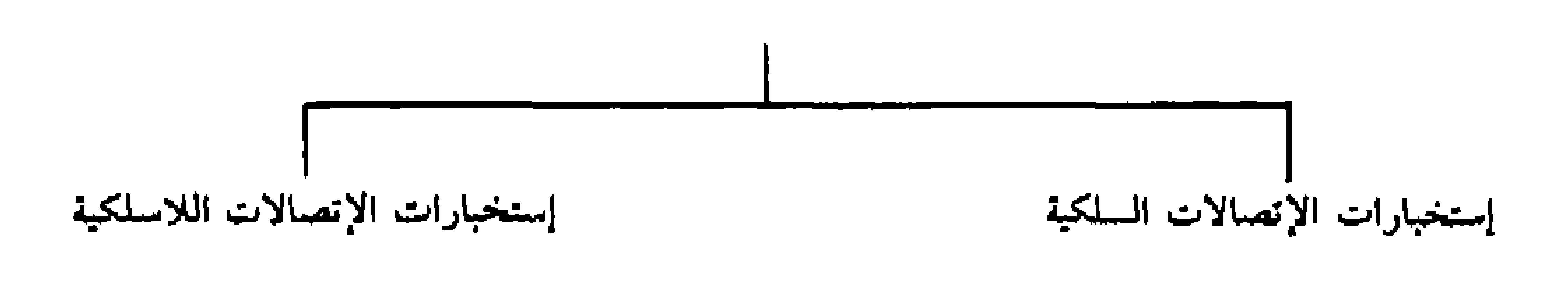
الرسالة
(TEXT)

البيانات
(DATA)

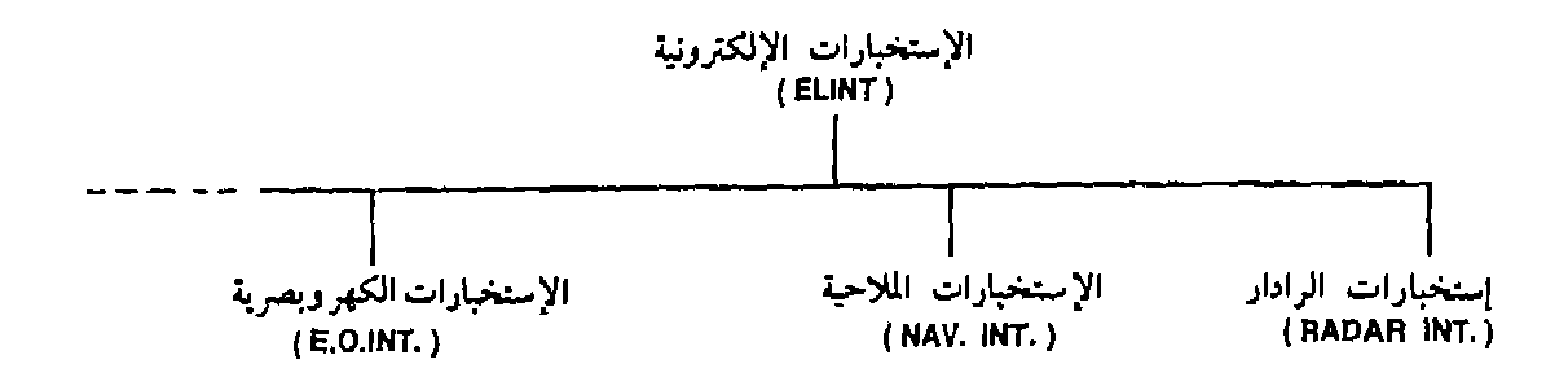
نقل الصور
(FAXIMILE)

٨ ـ وسط (إستخبارات الإتصالات):

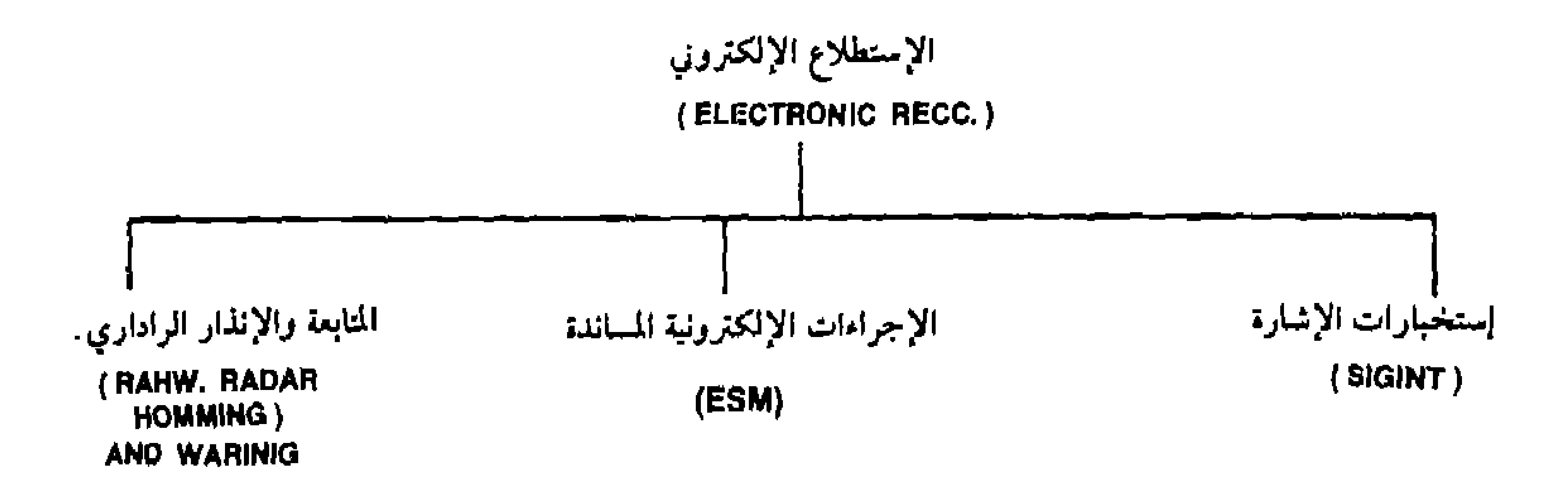
إستخبارات الإتصالات



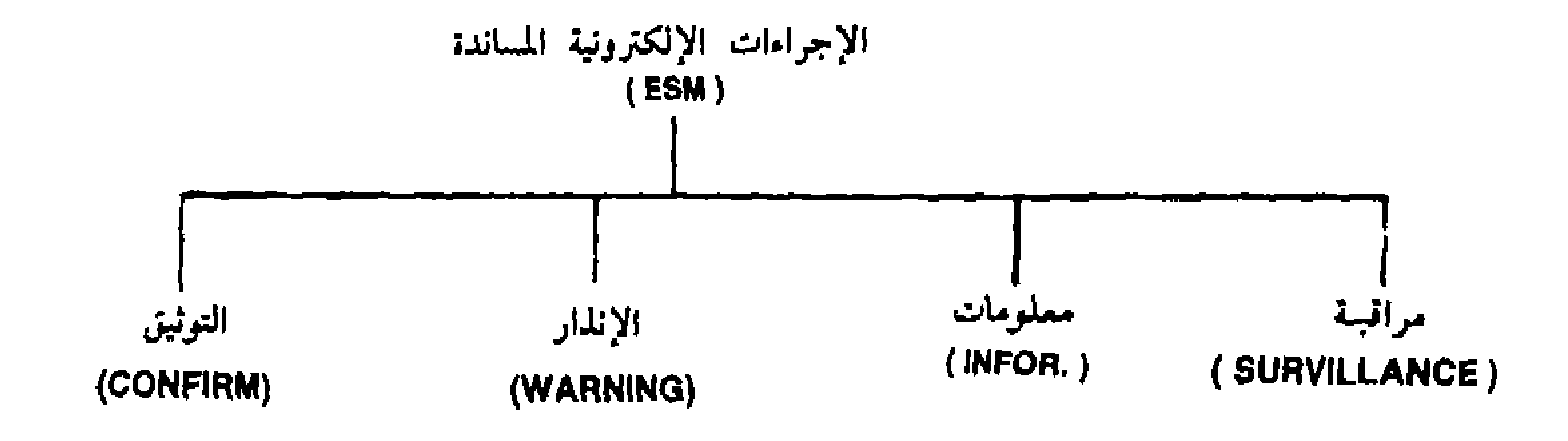
٩ ـ تقنيات (الإستخبارات الإلكترونية):



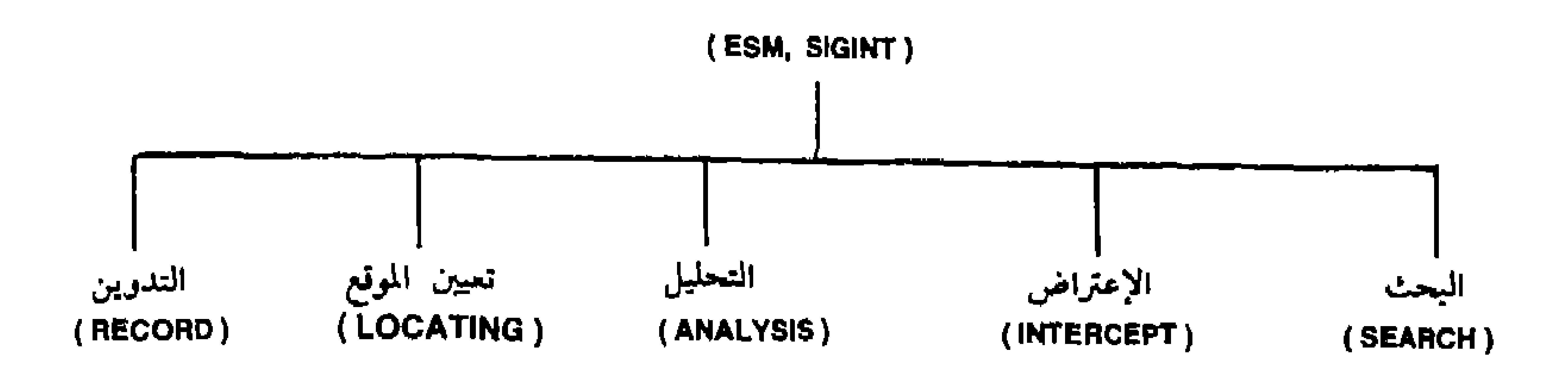
١٠ ـ أقسام الإستطلاع الإلكتروني:



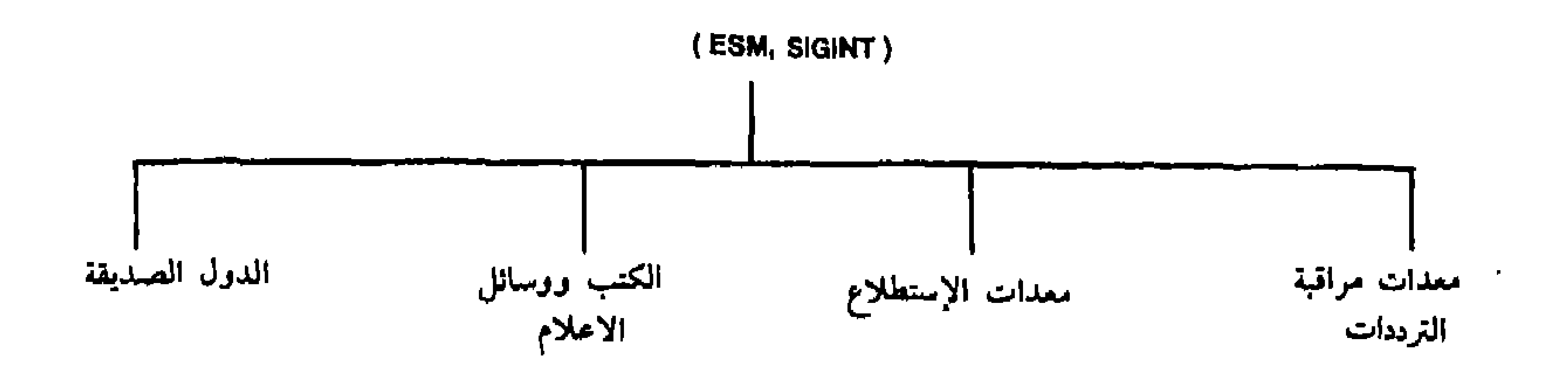
١١ ـ نتائج الإجراءات الإلكترونية المساندة :



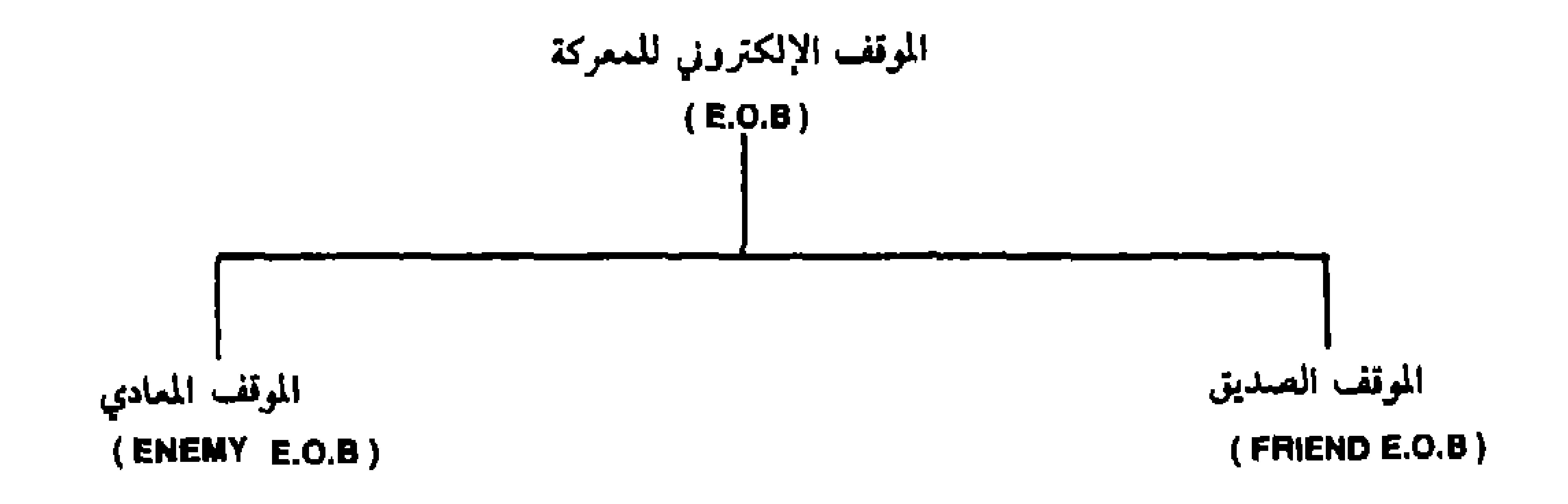
١٢ ـ خطوات الإجراءات الإلكترونية المساندة وإستخبارات الإشارة:



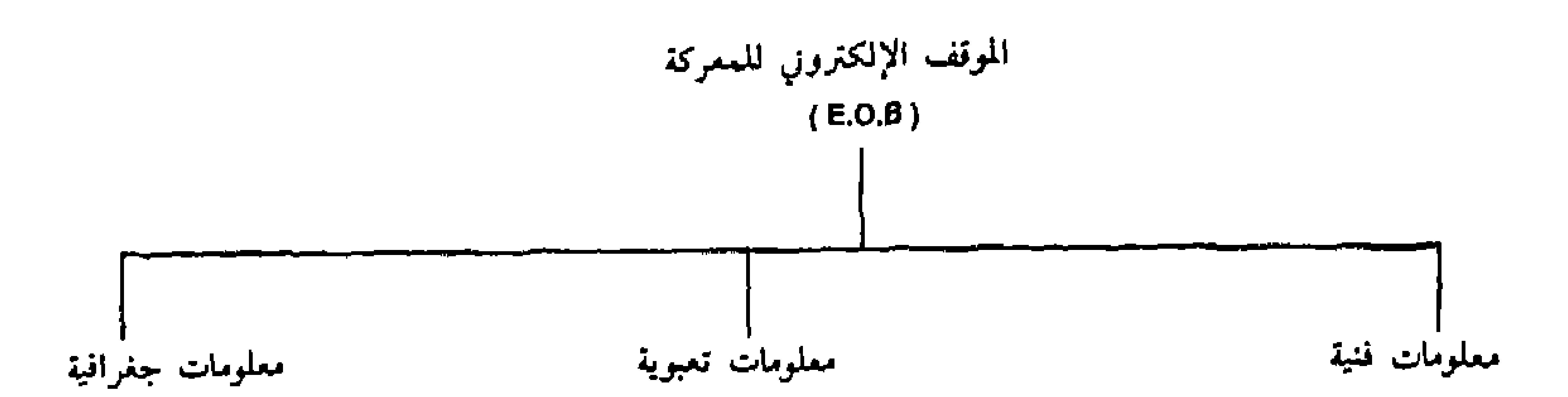
١٣ ـ مصادر الإجراءات الإلكترونية المساندة وإستخبارات الإشارة :



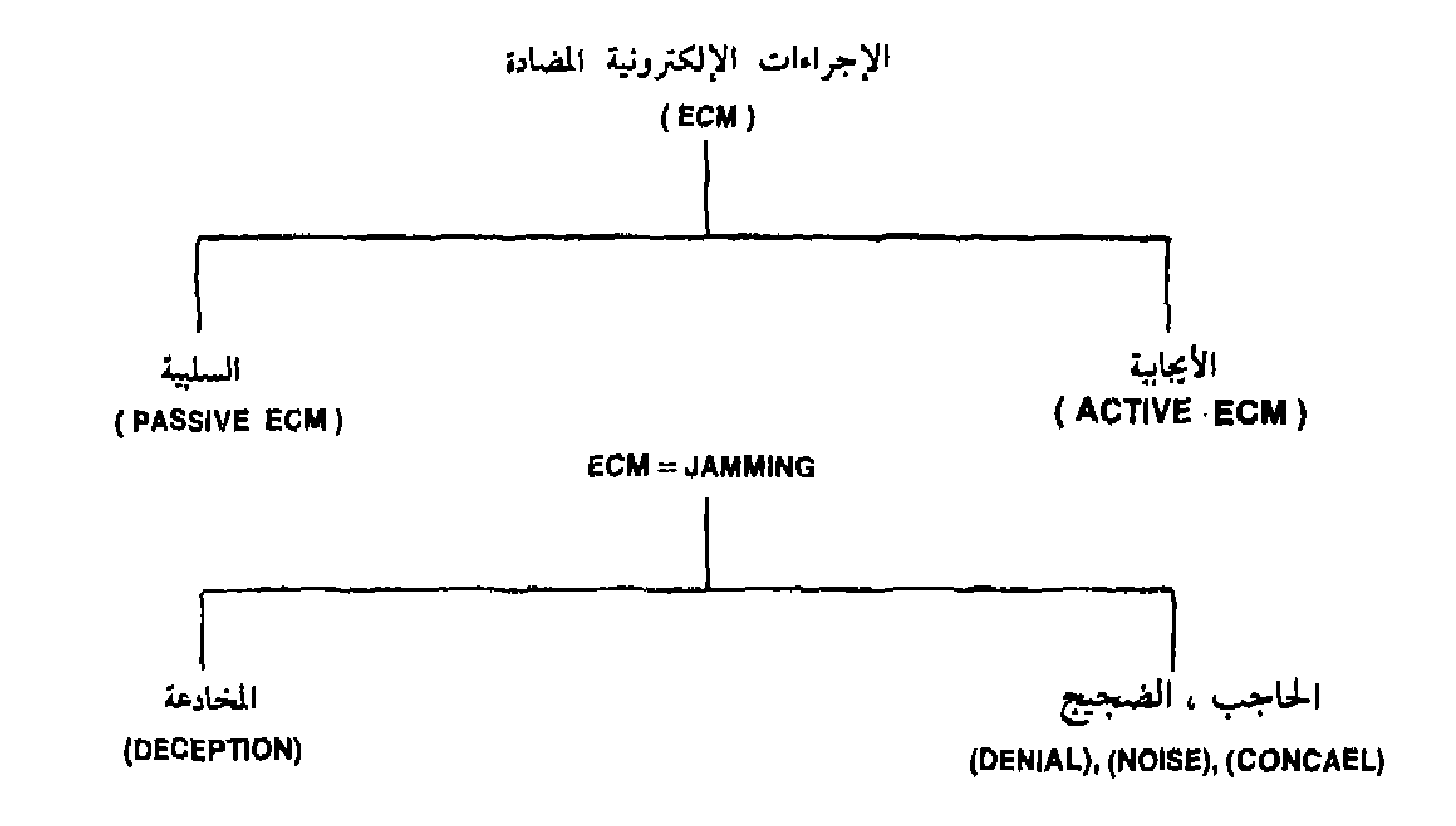
١٤ ـ مكونات الموقف الإلكتروني للمعركة :



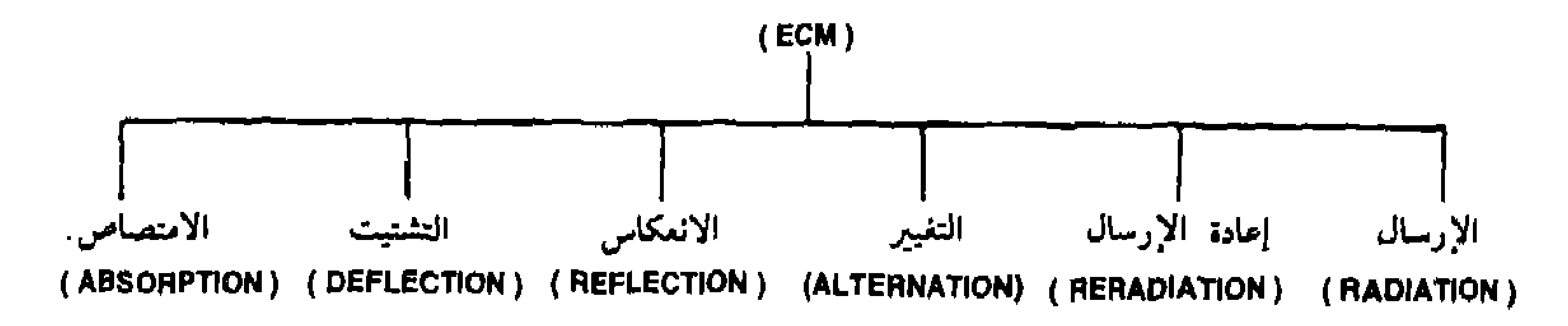
١٥ ـ معلومات الموقف الإلكتروني للمعركة :



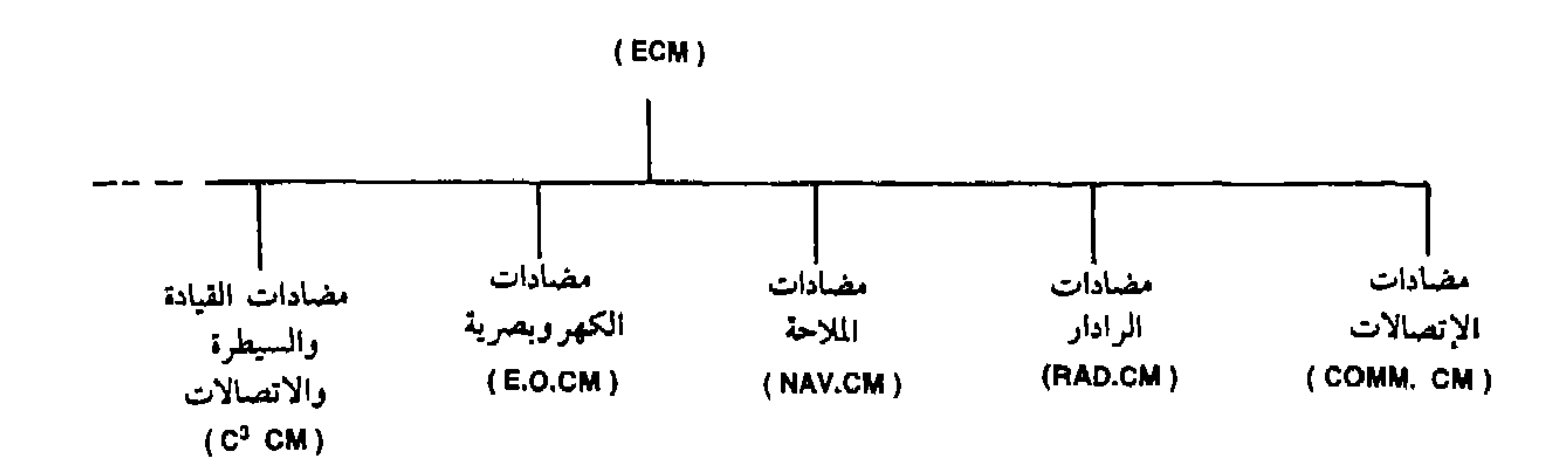
١٦ ـ معدات وأجهزة الإجراءات الإلكترونية المضادة :



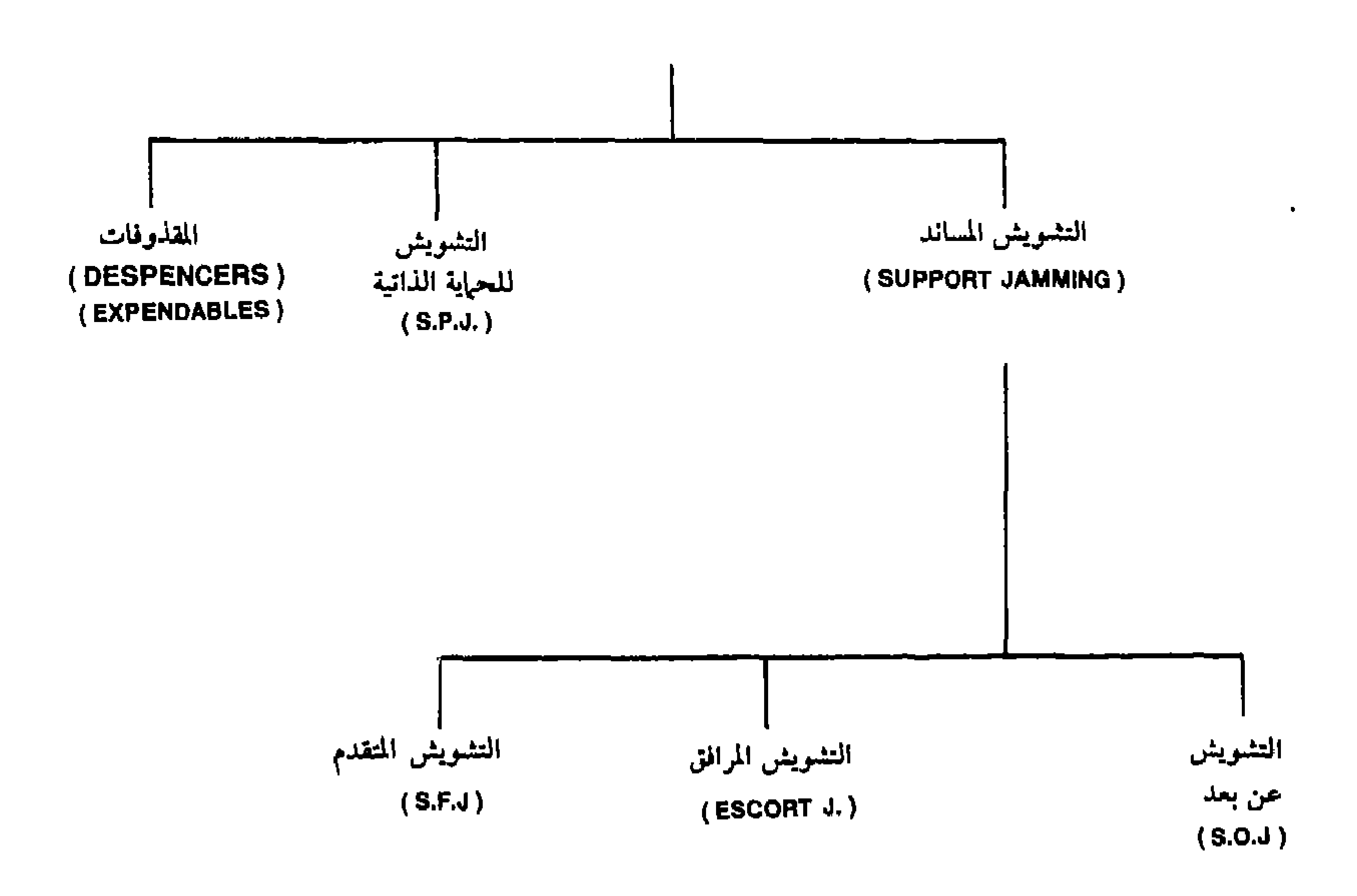
١٧ ـ نوعية الإجراءات الإلكترونية المضادة :



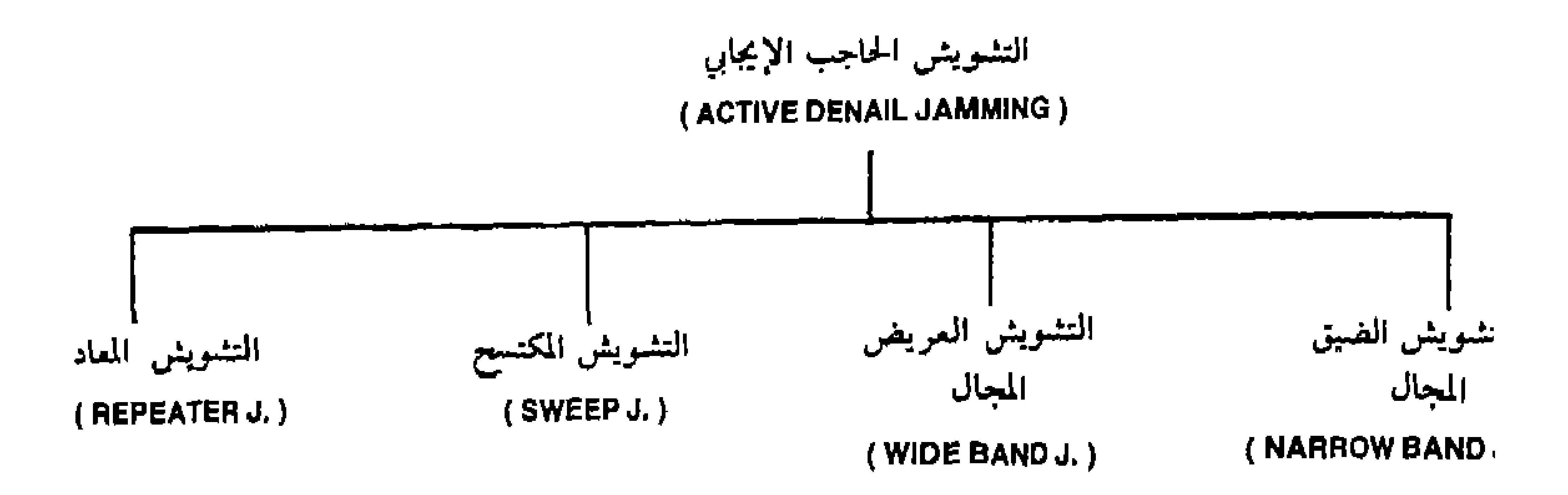
١٨ ـ تقنيات الإجراءات الإلكترونية المضادة :



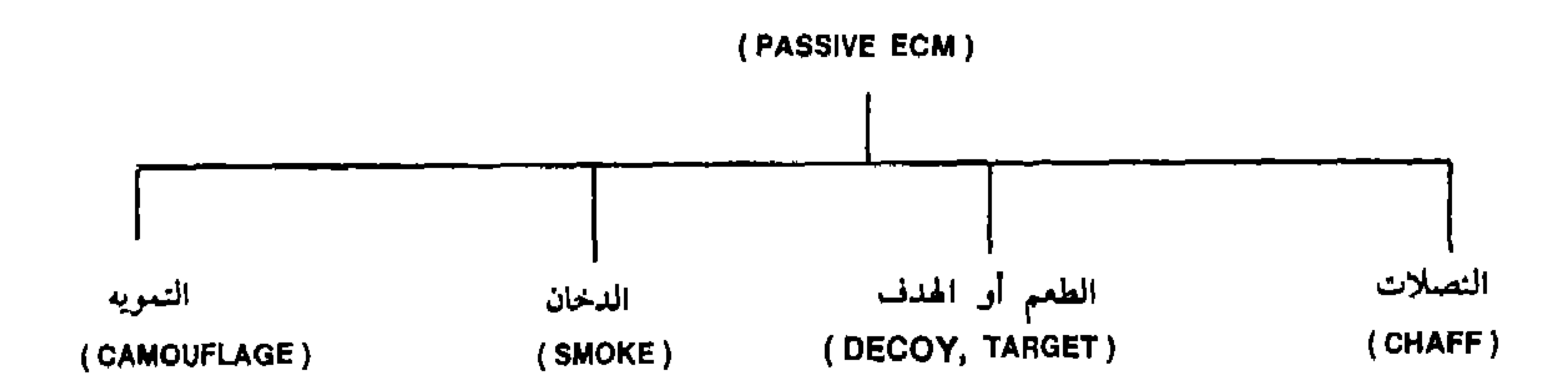
١٩ ـ أساليب الإجراءات الإلكترونية المضادة :



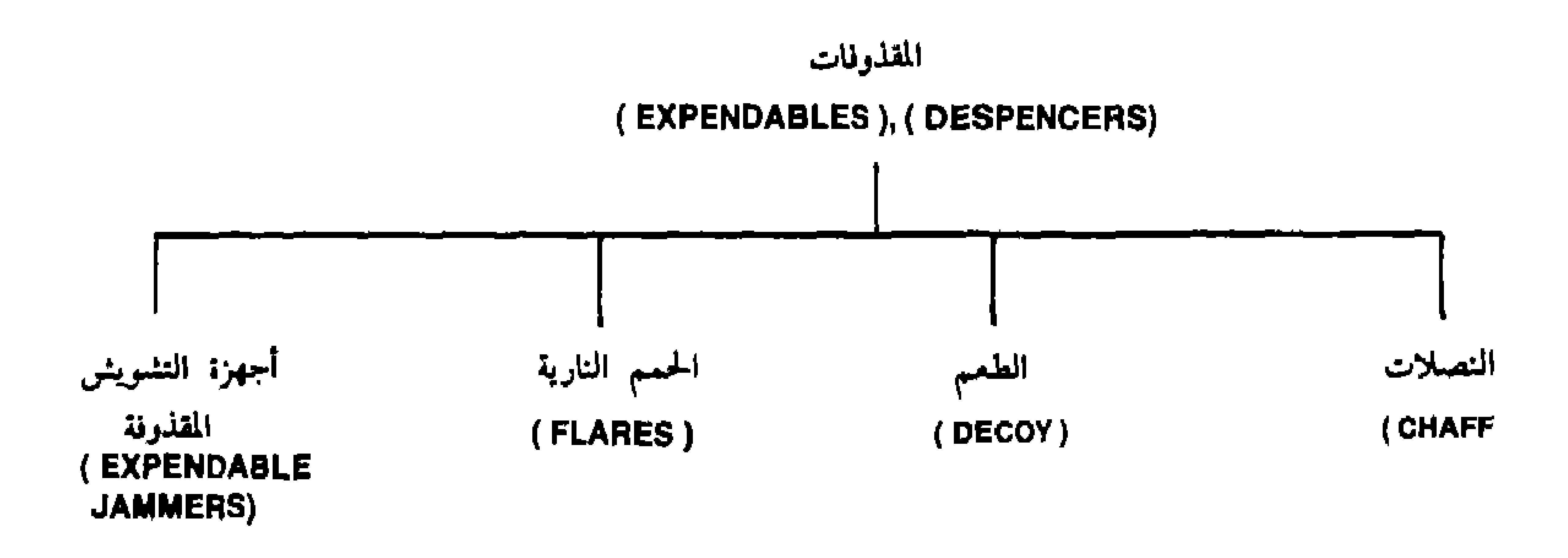
٢٠ ـ أنواع التشويش الحاجب الإيجابي :



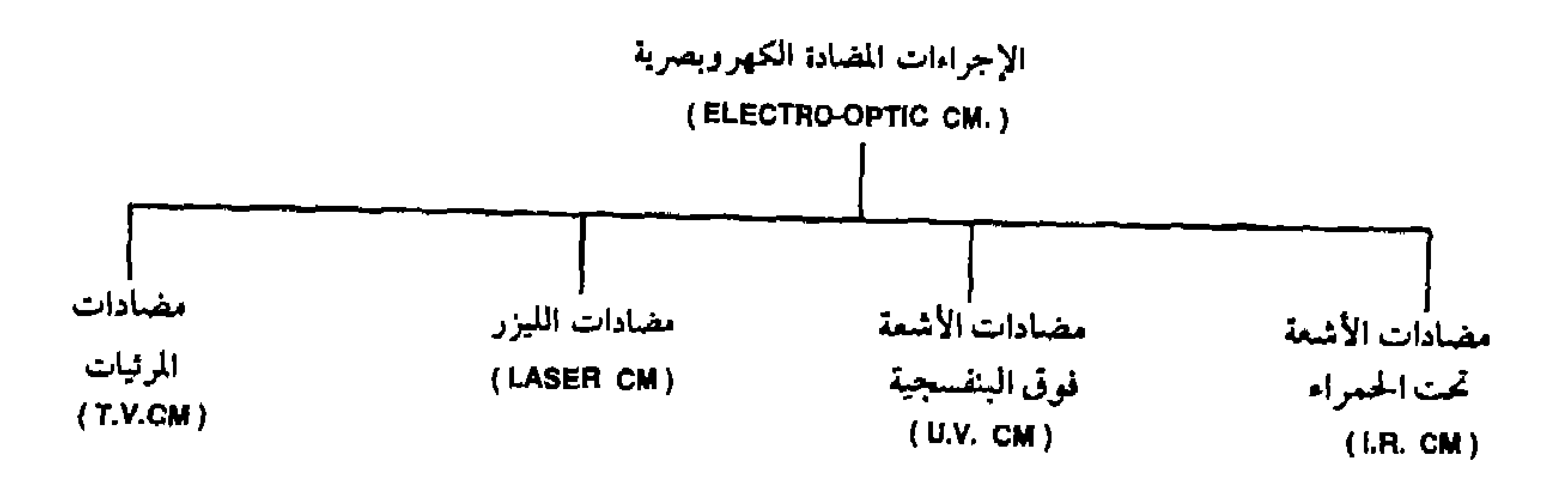
٢١ ـ تقنيات الإجراءات الإلكترونية المضادة السلبية :



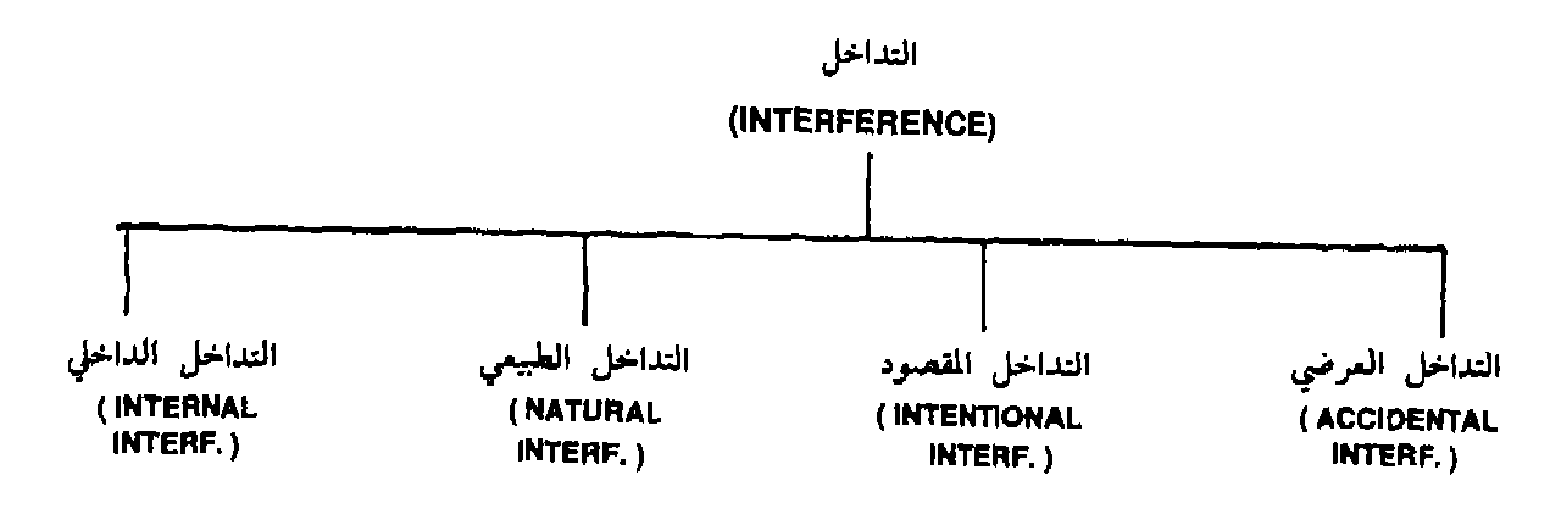
٢٢ ـ أنواع المقذوفات :



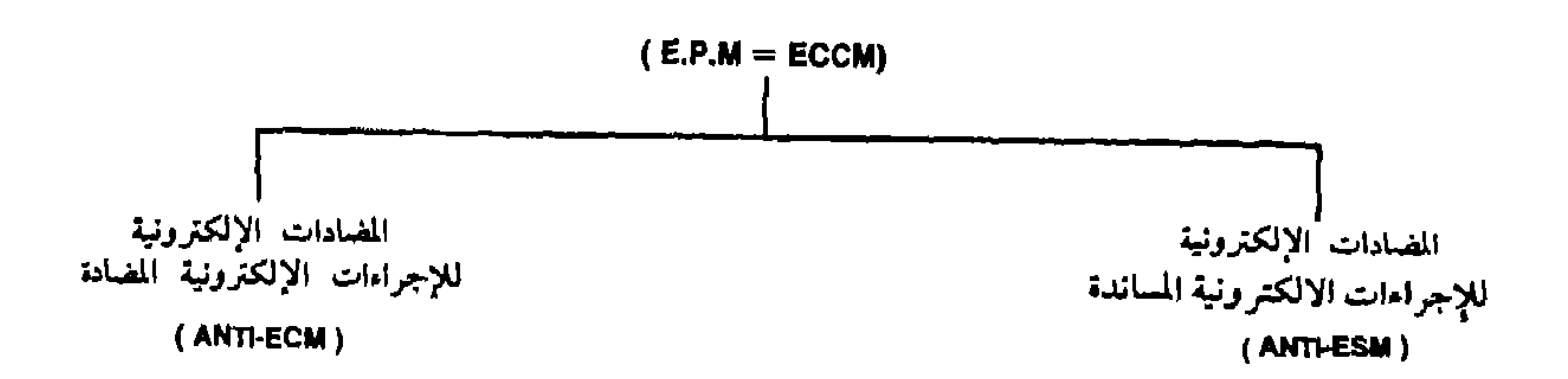
٢٣ ـ تقنيات الإجراءات المضادة الكهروبصرية :



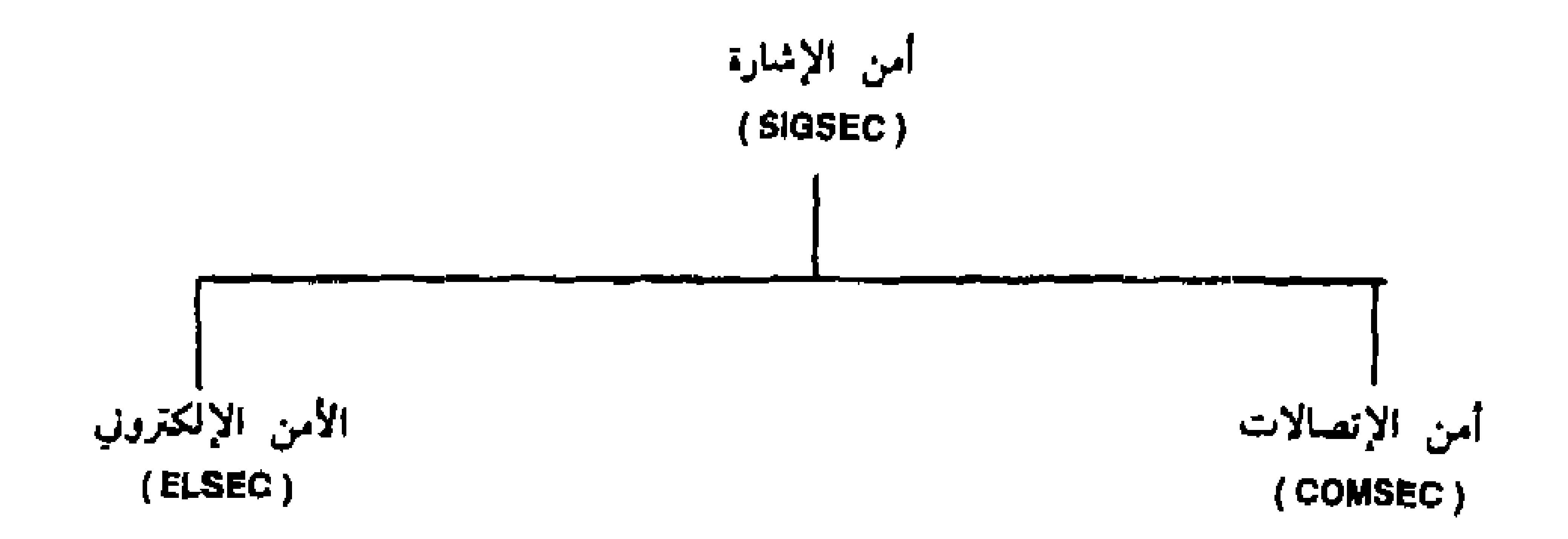
٢٤ ـ أنواع التداخل :



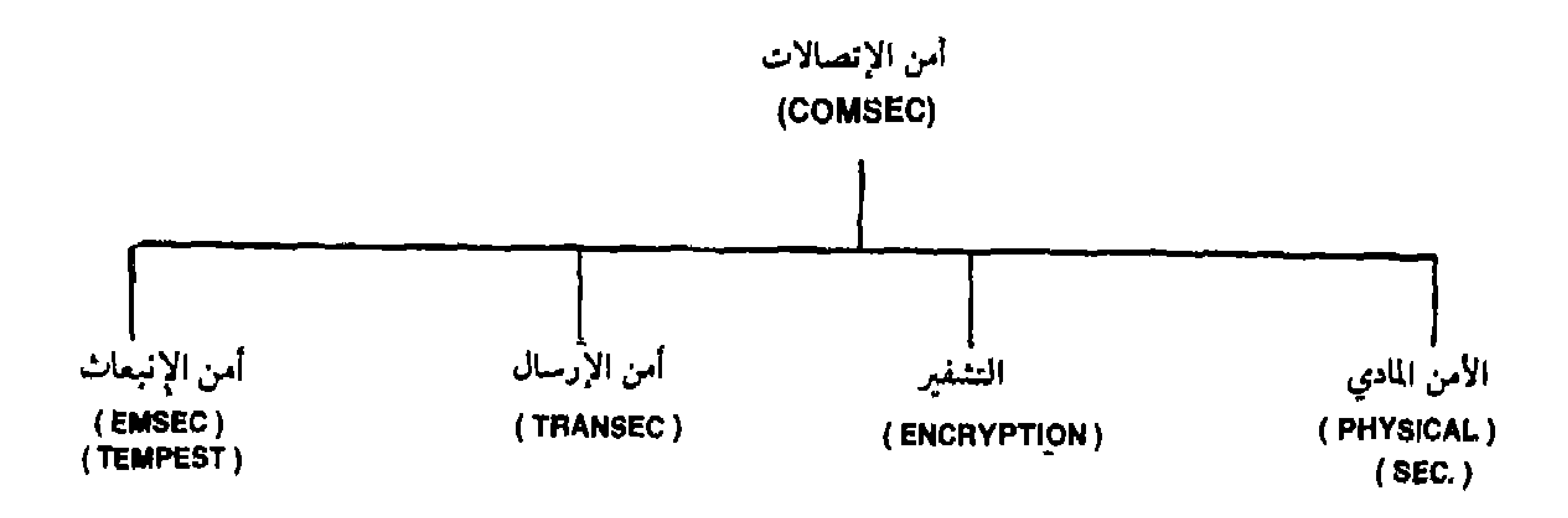
٢٥ ـ أقسام إجراءات الحماية الإلكترونية =
المضادات الإلكترونية للإجراءات المضادة :



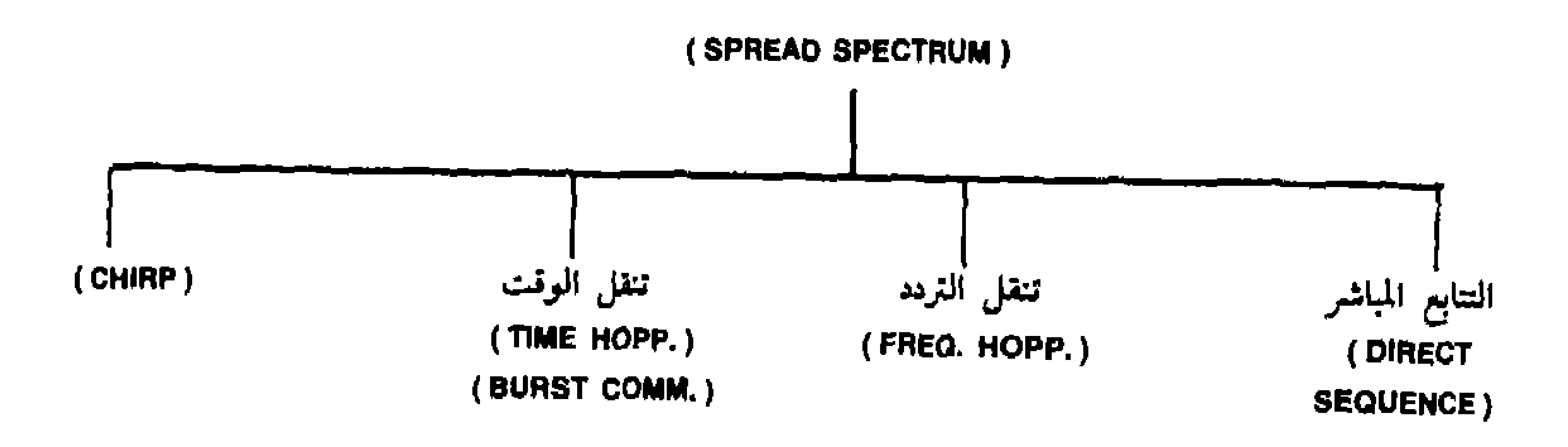
٢٦ ـ أقسام أمن الإشارة :



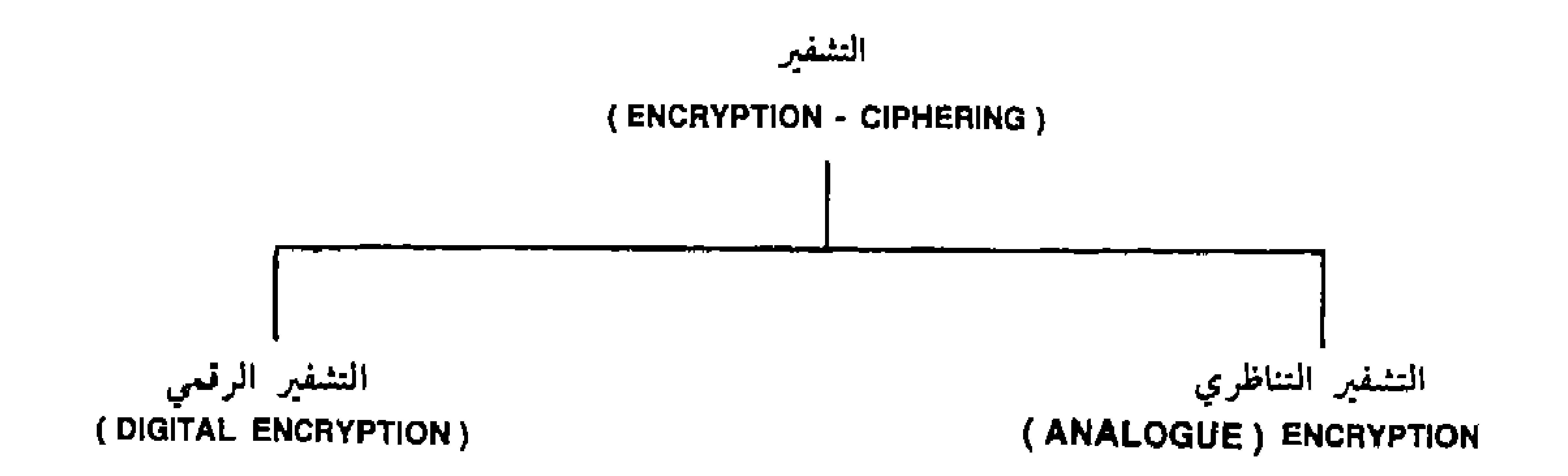
٢٧ ـ أقسام أمن الإتصالات :



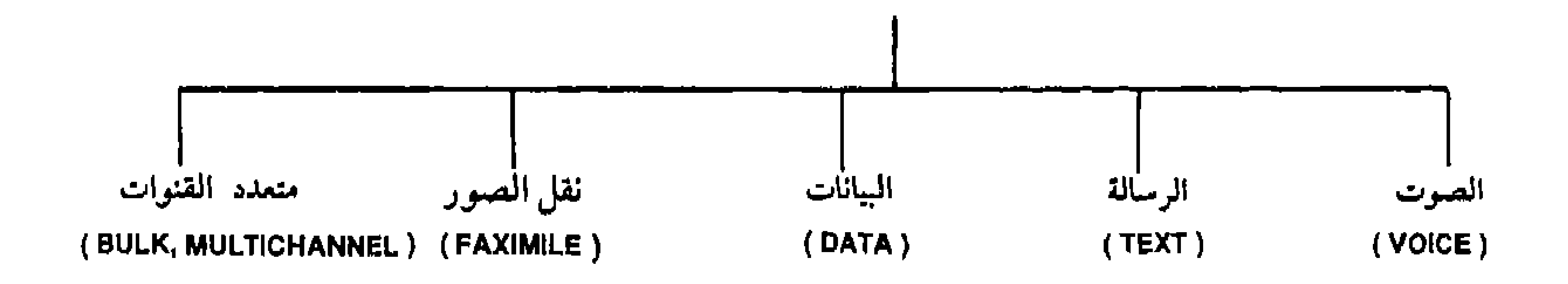
٢٨ ـ تقنيات الطيف الممتد :



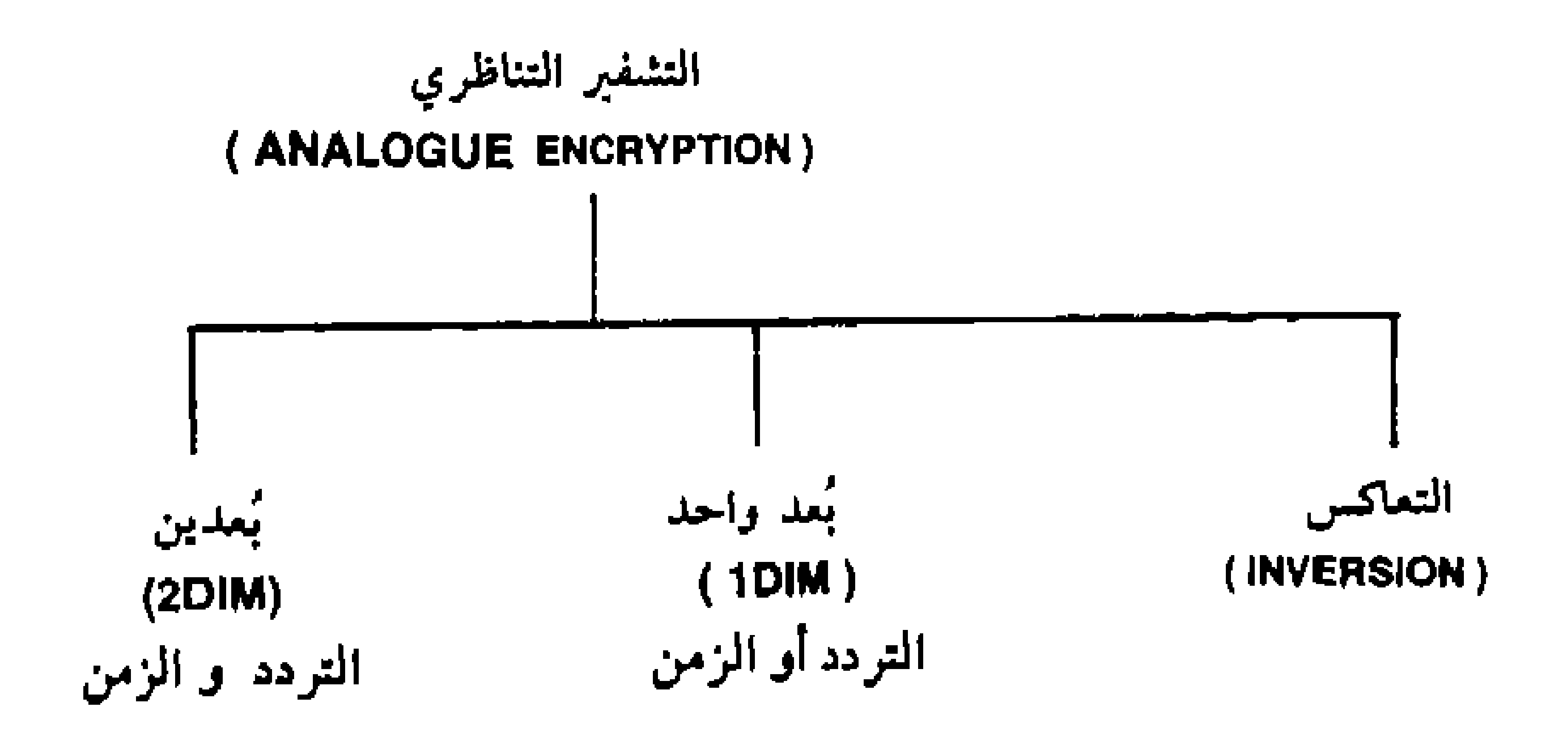
٢٩ ـ أنواع التشفير الإلكتروني :



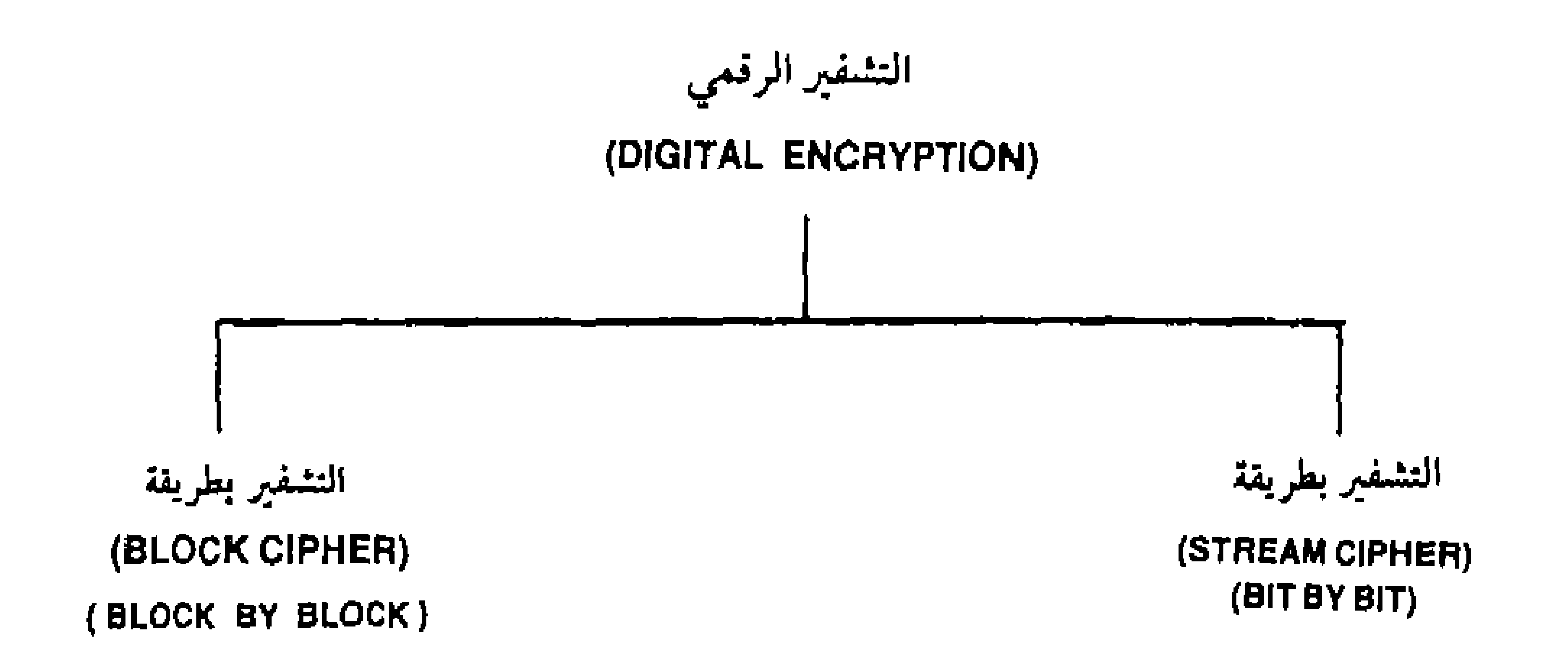
٣٠ ـ تستخدم أجهزة التشفير : لتشفير المعلومات والأجهزة التالية :



٣١ ـ تقنيات التشفير التناظري :



٣٢ ـ تقنيات التشفير الرقمي :



المراجع

أولاً : المراجع العربية :

١ ــ مجلة الوطن العربي (تصدر في باريس) ١/١٠/١٩٨٢ م .
٢ ــ مجلة المجلة (تصدر في لندن) ١٧/٥/١٩٨٤م.
٣ ــ كتاب الحرب الإلكترونية تأليف كمال السعدي (المركز العربي للدراسات الإستراتيجية) الطبعة الثانية مارس عام ١٩٧٩م. الناشر: المؤسسة العربية للدراسات والنشر (صندوق بريد ١١/٥٤٦٠ بيروت).
٤ ــ الموسوعة العسكرية (المؤسسة العربية للدراسات والنشر) طبعة عام ١٩٧٧م.
٥ ــ جريدة القبس الكويتية ٢٥/١٠/٨٤، ٣/١/١٩٨٥م.

ثانياً : المراجع الأجنبية :

1. FLIGHT INTERNATIONAL MAGAZINE
19/6/1982, 10/7/1982, 7/8/1982 21/8/1982, 26/5/1984, 9/3/1985

2. AVIATION WEEK AND SPACE TECHNOLOGY MAGAZINE.
14/6/1982, 5/7/1982

3. MILITARY TECHNOLOGY MAGAZINE.
7/1982, 6/1983, 10/1983, 3/1984, 6/1983

4. NATO'S FIFTEEN NATIONS MAGAZINE.
SPECIAL ISSUE 1/1982

5. COMMUNICATIONS INTERNATIONAL MAGAZINE.
10/1984

6. JANE'S DEFENCE WEEKLY MAGAZINE.
11/8/1985

7. INTERNATIONAL DEFENCE REVIEW MAGAZINE.
2/1976, 3/1976, E-W 5/1978, 6/1981, M.E. 1980

8. AIR FORCE MAGAZINE. (AMERICAN)
7/1982

9. THE INTERNATIONAL COUNTERMEASURES HANDBOOK.
(1977-1978), (1981-1982), (1985)-(1987).
PUBLISHED BY: W.W. COMMUNICATIONS INC.,
1170 EAST MEADOW DRIVE,PALOALTO,
CALIFORNIA 94303 U.S.A.

10. RADAR ELECTRONIC COUNTER-COUNTERMEASURES.
BY: STEPHEN L. JOHNSTON, SECOND PRINT 1980.
ARTECH HOUSE, INC.
610 WASHINGTON ST. DEDHAM, MA 02026 U.S.A.

11. INTELLIGENCE WARFARE
BY: COL. WILLIAM V. KENNEDY
1983 EDITION, PUBLISHED BY CRESENT BOOKS,
DISTRIBUTED BY CROWN PUBLISHERS, INC.
ONE PARK AVENUE, NEW YORK,
NEW YORK 10016, U.S.A.

12. WORLD ELECTRONIC WARFARE AIRCRAFT
BY: MARTIN STREETLY
FIRST PUBLISHED IN THE UNITED KINGDOM IN 1983
BY JANE'S PUBLISHING COMPANY LIMITED, 238 CITY
ROAD, LONDON EC1V 2PU.

13. INTRODUCTION TO RADAR SYSTEM
BY: MERRILL I. SKOLNIK
1980, SECOND EDITION
PUBLISHED BY McGRAW - HILL BOOK COMPANY.

14. HUGHES AIRCRAFT COMPANY
ELECTRONIC WARFARE
SEMINAR SUPPLEMENT
NO 355569-25(8-18-83)
U.S.A.

15. RACAL COMMUNICATIONS LIMITED
STRATEGIC RADIO SURVEILLANCE (PRUCHER)
PUBLICATION NO. 7079-5
BRACKNELL BERKSHIRE RG12G ENGLAND

16. AIRBORNE EARLY WARNING
BY MIKE HIRST
1983 EDITION, PUBLISHED BY OSPREY PUBLISHING LIMITED
12-14 LONG ACRE, LONDON WC2 E9LP, U.K.

17. ELECTRONIC COUNTER MEASURES
PUBLISHED BY PENINSULA PUBLISHING
P.O.BOX 867, LOS ALTOS, CALIFORNIA, 94022
U.S.A.

18. INTRODUCTION TO ELECTRONIC WARFARE
BY: D. CURTIS SCHLEHER, PH.D.
1986
ARTECH HOUSE, INC.
610 WASHINGTON STREET
DEDHAM, MA 02026 USA

19. ECM PRIMER
BY: ROBERT L. CAMPBELL
NO. SSE/ED 790627A
WATKINS-JOHNSON COMPANY
3333 HILLVIEW AVENUE
PALO ALTO, CALIFORNIA 94304 U.S.A.

هذا الكتاب

أخذت الحروب صوراً عديدة تطورت بتطور الزمن ، وتنوعت أساليبها ، وتعددت أشكالها ، واستمرت في تقدمها حتى وصلت إلى : « الحرب الإلكترونية » .

تُرى ما هي الحرب الإلكترونية ؟ وما هي أسسها ؟ وما معداتها ؟ وما أساليبها ؟ وما أهدافها ؟ وما أهميتها ؟ وما أثرها في الحروب الحديثة بصورة عامة ، وفي معارك الشرق الأوسط بصورة خاصة ؟

هذه الأسئلة وأسئلة أخرى غيرها استغرقت من المؤلف بحثاً عن إجاباتنا أكثر من ثلاث سنوات من الدراسة والتحليل حتى أثمرت هذا الكتاب .

وقد جاءت معلوماته مبسطة يسهل استيعابها على المتخصص وغير المتخصص .

ويعتبر الكتاب إضافة جديدة إلى المكتبة العربية ، يملأ منها ركناً لا يحوي مثيله .

الناشر

المؤسسة العربية
للدراسات والنشر
بناية برج الكارلتون ـ ساقية الجنزير ـ
ت ٨٠٧٩٠٠/١ برقياً « موكيالي » بيروت ـ
ص.ب ١١/٥٤٦٠ بيروت